

# DATA RECORDING DEVICE, DATA REPRODUCING DEVICE, DATA PROCESSING DEVICE AND DATA RECORDING MEDIUM

**Publication number:** JP2001332023 (A)

**Publication date:** 2001-11-30

**Inventor(s):** NONAKA SATOSHI; EZAKI TADASHI +

**Applicant(s):** SONY CORP +

**Classification:**

- international: **G06F12/14; G06F21/24; G10K15/02; G11B19/02; G11B20/10; G06F12/14; G06F21/00; G10K15/02; G11B19/02; G11B20/10; (IPC1-7): G11B19/02; G11B20/10**

- European:

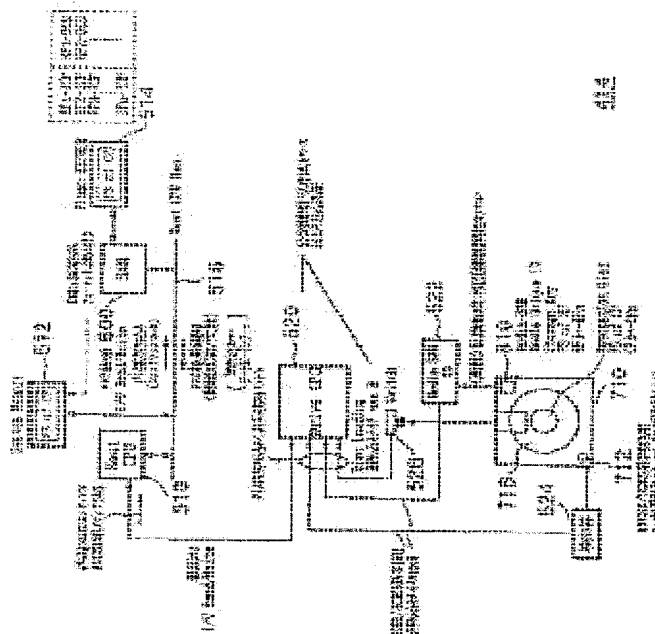
**Application number:** JP20000152788 20000519

**Priority number(s):** JP20000152788 20000519

## Abstract of JP 2001332023 (A)

**PROBLEM TO BE SOLVED:** To provide a recording device which records and reproduces data while adequately performing right processing and, a reproducing device, a data processing device for delivering the data and a recording medium.

**SOLUTION:** The data is encrypted and delivered and is subjected to the right processing by the secure processing means mounted at respective apparatus. The data is recorded and reproduced only in the case of the adequate right. The secure processing means having key data, authentication means, etc., are mounted at the recording medium as well and are subjected to interauthentication with the device side every time the means are mounted at the recording and reproducing device. Whether the device and medium have the adequate rights with each other or not is inspected. As to the data used by adequate right processing, use history information is previously stored and finally approval is effected by third party organizations.



Data supplied from the **espacenet** database — Worldwide

(11)特許出願公開番号

特開2001-332023

(P2001-332023A)

(43)公開日 平成13年11月30日(2001.11.30)

(51) Int.Cl.<sup>7</sup>

識別記号

FI

テーマコード\* (参考)

G 1 1 B 20/10  
19/02

501

G 1 1 B 20/10  
19/02

H	5 D 0 4 4
5 0 1 J	5 D 0 6 6

審査請求 未請求 請求項の数25 O L (全 32 頁)

(21)出願番号 特願2000-152788(P2000-152788)

(22)出願日 平成12年5月19日(2000.5.19)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 野中 聡

東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(72)発明者 江崎 正

東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(74)代理人 100094053

弁理士 佐藤 隆久

Fターム(参考) 5D044 CC04 DE49 DE50 EF05 FG18

GK17 HL08

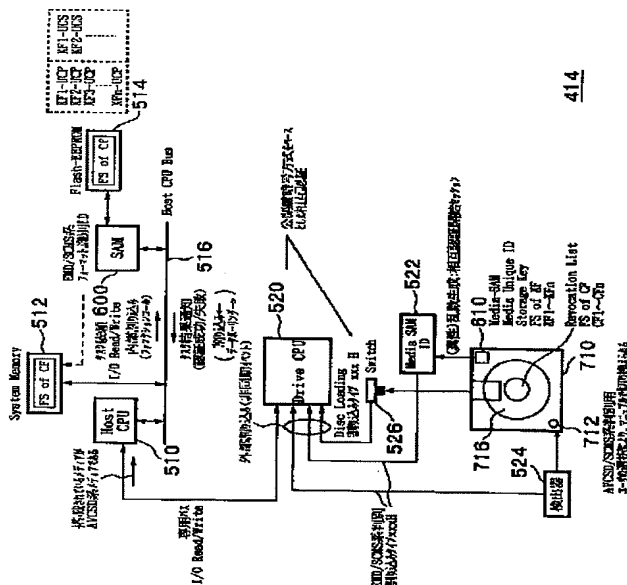
5D066 DA03 DA12 DA16

(54) 【発明の名称】 データ記録装置、データ再生装置、データ処理装置およびデータ記録媒体

(57) 【要約】

【課題】適切に権利処理を行いながらデータを記録再生する記録装置、再生装置、データを配信するデータ処理装置および記録媒体を提供する。

【解決手段】データは暗号化して配信し、各機器に搭載されたセキュアな処理手段で権利処理を行い、適切な権利の場合にのみ記録、再生を行なう。記録媒体にも、鍵データや認証手段などを有するセキュアな処理手段を搭載し、記録再生装置に搭載されるごとに、装置側と相互認証を行い、相互に適切な権利を有する装置、媒体であるか検査する。適切に権利処理して使用されたデータについては、使用履歴情報を蓄積しておき、最終的に第三者機関で決済を行なう。



## 【特許請求の範囲】

【請求項 1】装着された記録媒体が適切な処理対象の記録媒体か否かを検査する記録媒体検査手段と、前記記録媒体が適切な場合に、入力される暗号化された配信対象のデータを、入力される当該データの使用条件の範囲内で前記記録媒体に記録する記録手段と、前記記録に係わる係わる使用履歴情報を記憶する手段と、前記使用履歴情報を所定の送信先に送信する送信手段とを有するデータ記録装置。

【請求項 2】前記記録媒体検査手段は、前記データ記録媒体と相互認証を行なうことにより、当該データ記録媒体が適切な転送先か否かを検査する請求項 1 に記載のデータ記録装置。

【請求項 3】前記記録媒体検査手段は、前記データ記録媒体の所定のセキュアな記録領域より所定の識別情報を読み出し、該読み出した識別情報に基づいて当該データ記録媒体が適切な転送先か否かを検査する請求項 1 に記載のデータ記録装置。

【請求項 4】前記装着された前記記録媒体の所定の物理形状を検出する形状検出手段を有し、前記記録媒体検査手段は、前記検出された前記装着された記録媒体の所定の形状に基づいて、当該データ記録媒体が適切な転送先か否かを検査する請求項 1 に記載のデータ記録装置。

【請求項 5】前記記録媒体検査手段は、外部より観察不可能な状態で前記各処理を行なう請求項 3 に記載のデータ記録装置。

【請求項 6】前記記憶手段は、前記記録媒体が適切な場合に、入力される暗号化された配信対象のデータを利用するための鍵データをさらに記憶する請求項 1 に記載のデータ記録装置。

【請求項 7】前記記録媒体に記録された鍵データを読み出す鍵データ読み出し手段と、前記記録媒体に記録された暗号化された配信対象のデータを読み出すデータ読み出し手段と、前記鍵データに基づいて前記暗号化された配信対象のデータを復号化する復号化手段と、前記使用条件の情報に従って、前記復号化された配信対象のデータを再生する再生手段とをさらに有し、前記使用履歴情報記憶手段は、前記再生の履歴情報をさらに記憶する請求項 6 に記載のデータ記録装置。

【請求項 8】前記鍵データ読み出し手段は、前記読み出した鍵データを、外部より観察不可能なセキュアな記憶領域に記憶する請求項 7 に記載のデータ記録装置。

【請求項 9】前記使用条件の情報は、当該配信対象の使用許可条件、対価、権利処理情報、課金条件の少なくともいずれかを含み、前記使用手段は、前記制御情報に基づいて前記データを使用し、当該使用に係わる使用履歴情報を通知する請求

項 1 に記載のデータ記録装置。

【請求項 10】前記配信対象のデータは、音楽データ、画像データ、映像（動画）データ、オーディオデータおよび映像データを含むビデオデータ、コンピュータプログラムデータ、コンピュータデータを含むコンテンツデータのいずれかである請求項 1 に記載のデータ記録装置。

【請求項 11】装着された記録媒体が適切な処理対象の記録媒体か否かを検査する記録媒体検査手段と、

10 前記記録媒体が適切な場合に、前記記録媒体より鍵データを読み出す鍵データ読み出し手段と、

前記記録媒体が適切な場合に、前記記録媒体より暗号化された配信対象のデータを読み出すデータ読み出し手段と、

前記記録媒体が適切な場合に、前記記録媒体より前記配信対象のデータの使用条件の情報を読み出す使用条件読み出し手段と、前記鍵データに基づいて前記暗号化された配信対象のデータを復号化する復号化手段と、

20 前記使用条件の情報に従って、前記復号化された配信対象のデータを再生する再生手段と前記再生の履歴情報を記憶する使用履歴情報記憶手段と、前記記憶した使用履歴情報を所定の送信先に送信する送信手段とを有するデータ再生装置。

【請求項 12】配信される、暗号化された配信対象のデータと当該データの使用条件の情報を含む暗号化された配信データ、および、前記配信データを利用するための鍵データを、各々受信する受信手段と、

前記受信した配信データを蓄積する蓄積手段と、

30 前記受信した鍵データに基づいて、前記暗号化された配信データを復号化する復号化手段と、

前記復号化された配信データに含まれる使用条件の情報に従って、前記配信対象のデータを使用可能な状態とする第 1 の使用手段と、

任意のデータ転送先が、前記配信データの転送先として適切か否かを検査する転送先検査手段と、

前記検査の結果、前記データ転送先が適切であった場合に、少なくとも前記使用可能な状態とされた配信データを配信するデータ転送手段とを有するデータ処理装置。

40 【請求項 13】前記第 1 の使用手段における前記使用に係わる履歴情報を記憶する使用履歴情報記憶手段と、

前記記憶した使用履歴情報を所定の送信先に送信する送信手段とをさらに有する請求項 12 に記載のデータ処理装置。

【請求項 14】前記使用可能な状態とされた配信対象のデータを使用する第 2 の使用手段をさらに有する請求項 12 に記載のデータ処理装置。

【請求項 15】前記第 1 の使用手段および前記第 2 の使用手段における前記使用に係わる履歴情報を記憶する使用履歴情報記憶手段と、

50 前記記憶した使用履歴情報を所定の送信先に送信する送

信手段とをさらに有する請求項 13 に記載のデータ処理装置。

【請求項 16】前記復号手段、前記第 1 の使用手段、前記転送先検査手段、前記第 2 の使用手段および前記使用履歴情報記憶手段は、外部より観察不可能な状態で前記各処理を行なう請求項 15 に記載のデータ処理装置。

【請求項 17】前記データ転送先は、データ記録装置であって、

前記転送先検査手段は、前記データ記録装置と相互認証を行なうことにより、当該データ記録装置が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録装置が適切であった場合に、前記使用可能な状態とされた前記配信データを配信する請求項 13 に記載のデータ処理装置。

【請求項 18】前記データ転送先は、データ記録媒体であって、

前記転送先検査手段は、前記データ記録媒体と相互認証を行なうことにより、当該データ記録媒体が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録媒体が適切であった場合に、前記使用可能な状態とされた前記配信データを当該データ記録媒体に記録する請求項 13 に記載のデータ処理装置。

【請求項 19】前記データ転送先は、データ記録媒体であって、

前記転送先検査手段は、前記データ記録媒体の所定のセキュアな記録領域より所定の識別情報を読み出し、該読み出した識別情報に基づいて当該データ記録媒体が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録媒体が適切であった場合に、前記使用可能な状態とされた前記配信データを当該データ記録媒体に記録する請求項 13 に記載のデータ処理装置。

【請求項 20】配信される、暗号化された配信対象のデータと当該データの使用条件の情報を含む暗号化された配信データ、および、前記配信データを利用するための鍵データを、各々受信する受信手段と、

前記受信した配信データを蓄積する蓄積手段と、

任意のデータ転送先が、前記配信データの転送先として適切か否かを検査する転送先検査手段と、

前記検査の結果、前記データ転送先が適切であった場合に、少なくとも前記配信データを配信するデータ転送手段とを有するデータ処理装置。

【請求項 21】前記転送先検査手段は、外部より観察不可能な状態で、前記データ転送先が前記配信データの転送先として適切か否かを検査する請求項 20 に記載のデータ処理装置。

【請求項 22】前記データ転送先は、データ記録装置であって、

前記転送先検査手段は、前記データ記録装置と相互認証

を行なうことにより、当該データ記録装置が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録装置が適切であった場合に、前記配信データを配信する請求項 21 に記載のデータ処理装置。

【請求項 23】前記データ転送先は、データ記録媒体であって、

前記転送先検査手段は、前記データ記録媒体と相互認証を行なうことにより、当該データ記録媒体が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録媒体が適切であった場合に、前記配信データを当該データ記録媒体に記録する請求項 21 に記載のデータ処理装置。

【請求項 24】前記データ転送先は、データ記録媒体であって、

前記転送先検査手段は、前記データ記録媒体の所定のセキュアな記録領域より所定の識別情報を読み出し、該読み出した識別情報に基づいて当該データ記録媒体が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録媒体が適切であった場合に、前記配信データを当該データ記録媒体に記録する請求項 21 に記載のデータ処理装置。

【請求項 25】任意のデータを記録するデータ記録領域と、

装着されたデータ処理装置と通信を行い相互認証を行なう相互認証手段と、

前記認証の結果適切と判定されたデータ処理装置にのみアクセスされるデータを記録するデータ記録手段とを有するデータ記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、たとえば、音声や映像など種々の種類の信号、種々の仕様の機器、種々の信号諸元あるいは種々の権利関係などが混在し、ネットワークやパッケージメディアなど種々の媒体を介して配信されるデータ配信システムにおいて用いて好適な、データ記録装置、データ再生装置、データ処理装置およびデータ記録媒体に関する。

【0002】

【従来の技術】デジタル信号処理技術の急速な進展により、音楽データなどはデジタル信号として扱われ、MD や DVD などに記録され、利用されるようになっていく。さらに、これまでデータ量が膨大になるため敬遠されていた画像データも、デジタルデータとして扱われ、ランダムアクセス可能なディスク型の記録媒体や半導体メモリを用いた記録媒体に記録されるようになりつつある。一方で、通信技術および情報処理技術の進展により、インターネットを初めとする通信ネットワークの普及も著しい。そして、近年の通信速度や端末装置の性能の飛躍的な向上により、そのような通信ネットワークに

においては、個人間のメール転送やニュースの配信というような利用形態にとどまらず、前述したようなデジタル形式の音楽データ、ビデオデータあるいはコンピュータプログラムデータなどを配信できる環境となっている。

#### 【0003】

【発明が解決しようとする課題】ところで、そのようなデジタル形式の音楽データやビデオデータは、コピーを行なっても品質が劣化しないことから、著作権などを無視した不正なコピーが次々と行なわれる危険性がある。したがって、前述したようなネットワークを介したデータ配信においても、適切にデータの使用がコントロールされ、データの使用に基づく利益が適切に権利者に還元されるような仕組みを作ることが重要である。

【0004】したがって、本発明の目的は、所望のデータを、適切に権利処理を行いながら記録することのできるデータ記録装置を提供することにある。また本発明の目的は、記録された所望のデータを、適切に権利処理を行いながら再生することのできるデータ再生装置を提供することにある。また、本発明の他の目的は、所望のデータを、任意の信号諸元で任意の媒体、通信路、機器を介して任意の配信先に所定の権利処理を行いながら配信するためのデータ処理装置を提供することにある。さらに本発明の他の目的は、所望のデータを、適切に権利処理を行いながら記録および再生することのできるデータ記録媒体を提供することにある。

#### 【0005】

【課題を解決するための手段】したがって、本発明のデータ記録装置は、装着された記録媒体が適切な処理対象の記録媒体か否かを検査する記録媒体検査手段と、前記記録媒体が適切な場合に、入力される暗号化された配信対象のデータを、入力される当該データの使用条件の範囲内で前記記録媒体に記録する記録手段と、前記記録に係わる係わる使用履歴情報を記憶する手段と、前記使用履歴情報を所定の送信先に送信する送信手段とを有する。

【0006】好適には、前記記録媒体検査手段は、前記データ記録媒体と相互認証を行なうことにより、当該データ記録媒体が適切な転送先か否かを検査する。また好適には、前記記録媒体検査手段は、前記データ記録媒体の所定のセキュアな記録領域より所定の識別情報を読み出し、該読み出した識別情報に基づいて当該データ記録媒体が適切な転送先か否かを検査する。また好適には、前記装着された前記記録媒体の所定の物理形状を検出する形状検出手段を有し、前記記録媒体検査手段は、前記検出された前記装着された記録媒体の所定の形状に基づいて、当該データ記録媒体が適切な転送先か否かを検査する。さらに好適には、前記記録媒体検査手段は、外部より観察不可能な状態で前記各処理を行なう。

【0007】また好適には、前記記憶手段は、前記記録媒体が適切な場合に、入力される暗号化された配信対象

のデータを利用するための鍵データをさらに記憶する。また好適には、前記記録媒体に記録された鍵データを読み出す鍵データ読み出し手段と、前記記録媒体に記録された暗号化された配信対象のデータを読み出すデータ読み出し手段と、前記鍵データに基づいて前記暗号化された配信対象のデータを復号化する復号化手段と、前記使用条件の情報に従って、前記復号化された配信対象のデータを再生する再生手段とをさらに有し、前記使用履歴情報記憶手段は、前記再生の履歴情報をさらに記憶する。好適には、前記鍵データ読み出し手段は、前記読み出した鍵データを、外部より観察不可能なセキュアな記憶領域に記憶する。

【0008】特定的には、前記使用条件の情報は、当該配信対象の使用許可条件、対価、権利処理情報、課金条件の少なくともいずれかを含み、前記使用手段は、前記制御情報に基づいて前記データを使用し、当該使用に係わる使用履歴情報を通知する。また特定的には、前記配信対象のデータは、音楽データ、画像データ、映像（動画像）データ、オーディオデータおよび映像データを含むビデオデータ、コンピュータプログラムデータ、コンピュータデータを含むコンテンツデータのいずれかである。

【0009】また本発明のデータ再生装置は、装着された記録媒体が適切な処理対象の記録媒体か否かを検査する記録媒体検査手段と、前記記録媒体が適切な場合に、前記記録媒体より鍵データを読み出す鍵データ読み出し手段と、前記記録媒体が適切な場合に、前記記録媒体より暗号化された配信対象のデータを読み出すデータ読み出し手段と、前記記録媒体が適切な場合に、前記記録媒体より前記配信対象のデータの使用条件の情報を読み出す使用条件読み出し手段と、前記鍵データに基づいて前記暗号化された配信対象のデータを復号化する復号化手段と、前記使用条件の情報に従って、前記復号化された配信対象のデータを再生する再生手段と前記再生の履歴情報を記憶する使用履歴情報記憶手段と、前記記憶した使用履歴情報を所定の送信先に送信する送信手段とを有する。

【0010】また、本発明のデータ処理装置は、配信される、暗号化された配信対象のデータと当該データの使用条件の情報を含む暗号化された配信データ、および、前記配信データを利用するための鍵データを、各々受信する受信手段と、前記受信した配信データを蓄積する蓄積手段と、前記受信した鍵データに基づいて、前記暗号化された配信データを復号化する復号化手段と、前記復号化された配信データに含まれる使用条件の情報に従って、前記配信対象のデータを使用可能な状態とする第1の使用手段と、任意のデータ転送先が、前記配信データの転送先として適切か否かを検査する転送先検査手段と、前記検査の結果、前記データ転送先が適切であった場合に、少なくとも前記使用可能な状態とされた配信デ

ータを配信するデータ転送手段とを有する。

【0011】また、本発明の他のデータ処理装置は、配信される、暗号化された配信対象のデータと当該データの使用条件の情報を含む暗号化された配信データ、および、前記配信データを利用するための鍵データを、各々受信する受信手段と、前記受信した配信データを蓄積する蓄積手段と、任意のデータ転送先が、前記配信データの転送先として適切か否かを検査する転送先検査手段と、前記検査の結果、前記データ転送先が適切であった場合に、少なくとも前記配信データを配信するデータ転送手段とを有する。

【0012】また、本発明のデータ記録媒体は、任意のデータを記録するデータ記録領域と、装着されたデータ処理装置と通信を行い相互認証を行なう相互認証手段と、前記認証の結果適切と判定されたデータ処理装置にのみアクセスされるデータを記録するデータ記録手段とを有する。

#### 【0013】

【発明の実施の形態】本発明の一実施の形態について、図1～図46を参照して説明する。本実施の形態においては、音楽データを処理する装置であって、ネットワークを介して配信される音楽データを受信し利用可能な状態するデータ処理装置、そのような音楽データの利用装置としてのデータ記録装置、データ再生装置およびデータ記録再生装置などを例示して、本発明を説明する。なおここでは、本発明に係わる、音楽データを適正に利用するための権利処理や構成を中心に説明する。したがって、通常の音楽データの記録あるいは再生装置が有する通常の構成については、その詳細な説明を省略する。

#### 【0014】EMDシステム

まず、本発明に係わる各装置が使用される環境であり、音楽データをネットワークあるいはパッケージメディアを介して、適正な権利処理を行いながら配信する電子音楽配信システム（EMD（Electronic Music Distribution）システム）について説明する。

#### 【0015】EMDシステムの構成

まず、そのEMDシステム1の全体構成について図1を参照して説明する。図1は、そのEMDシステム1の構成を示すブロック図である。EMDシステム1は、EMDサービスセンタ100、コンテンツプロバイダ200、サービスプロバイダ250、デリバリチャネル300、ユーザホームネットワーク400を有する。なお、図1に示すEMDシステム1は、EMDサービスセンタ100、コンテンツプロバイダ200およびサービスプロバイダ250を各々1つ、ユーザホームネットワーク400を2つ有する構成であるが、これは説明に好適な構成であって、後に各々説明するように、各構成部の数は各々任意でよい。

#### 【0016】EMDサービスセンタ100

EMDサービスセンタ100は、音楽コンテンツデータ

が、適切に権利処理され、適切に課金処理され、そして適切に利益分配されながら適切に配信されるように、EMDシステム1全体を管理する。

【0017】具体的には、まずEMDサービスセンタ100は、コンテンツプロバイダ200、サービスプロバイダ250、ユーザホームネットワーク400のユーザおよび各機器を初めとして、メディアや図示せぬポータルなど、音楽コンテンツデータの配信に関わる全てのエンティティについて、それらの登録を受け付け、IDを割り当て、種々の属性や後の利益分配に用いる決済口座の口座番号などの情報をデータベースとして蓄積し管理する。特に、本発明に係わる、SAMを実質的に搭載しセキュアな状態で権利処理が可能となっているEMDシステム対応機器（以後、EMDハードウェアと言う場合もある。）については、基本的にその全ての機器の情報がEMDサービスセンタ100に登録され管理される。

【0018】またEMDサービスセンタ100は、それら各エンティティが、たとえばデータを伝送する際に用いる鍵データや証明書データなどを管理し、それらの正当性を証明する処理などを行なう。またEMDサービスセンタ100は、コンテンツプロバイダ200にコンテンツを暗号化して配信するためのディストリビューション鍵を配付するとともに、ユーザホームネットワーク400にその暗号を解読するためのディストリビューション鍵を適正な権利処理を条件に使用できる状態で配付することにより、コンテンツの配信をコントロールする。

【0019】またEMDサービスセンタ100は、コンテンツプロバイダ200より、配信対象の音楽コンテンツデータに関わる情報、その各音楽コンテンツデータごとの配信に関わった各エンティティに対する利益分配の割合を示す利益分配データ、および、その各音楽コンテンツデータの配信の際の信号諸元に対応した価格を規定した価格換算データの登録を受け付け、これらを管理する。そしてEMDサービスセンタ100は、ユーザホームネットワーク400からコンテンツの利用に応じて逐次送信されるコンテンツ使用情報（Usage-Log）を受信し、前述した利益分配データおよび価格換算データを参照して、そのコンテンツの制作から流通に係わった各エンティティへの利益の配分処理を行なう。

【0020】なお、このEMDサービスセンタ100は、各EMDシステム1ごとに1つ存在するのが好適である。

#### 【0021】コンテンツプロバイダ200

コンテンツプロバイダ200は、基本的に音楽コンテンツデータの著作権者であり、配信対象の配信コンテンツデータに対して、図2に示すようなコンテンツプロバイダセキュアコンテナを生成し、配信業者であるサービスプロバイダ250に供給する。具体的には、コンテンツプロバイダ200は、コンテンツデータに、自己のコンテンツであることを証明するための著作権情報をウォー

ターマーク情報（電子透かし情報）として重畳し、さらに、アナログインターフェイス経由でのコピーを禁止するためのコピー禁止ビットが埋め込まれているウォーターマーク情報を重畳し、そのコンテンツデータを圧縮して、自らが生成したコンテンツ鍵で暗号化する。

【0022】また、そのコンテンツに関する取扱方針を定めた使用許諾条件（UCP: Usage Control Policy）を作成し、EMDサービスセンタ100から配信されたディストリビューション鍵でコンテンツ鍵およびUCPを暗号化する。そして、コンテンツ鍵で暗号化されたコンテンツと、ディストリビューション鍵で暗号化されたコンテンツ鍵とUCPに対して、各々ハッシュ値をとり、コンテンツプロバイダ200の秘密鍵を用いて署名を生成する。この署名を、先の各データに添付してコンテンツプロバイダセキュアコンテナを生成し、サービスプロバイダ250に供給する。

【0023】また、コンテンツプロバイダ200は、コンテンツプロバイダセキュアコンテナを生成して音楽コンテンツデータを配信対象としたら、その音楽コンテンツデータに関わる情報、その各音楽コンテンツデータごとの配信に関わった各エンティティに対する利益分配の割合を示す利益分配データ、および、その各音楽コンテンツデータの配信の際の信号諸元に対応した価格を規定した価格換算データをEMDサービスセンタ100に送信し、登録する。登録した情報およびデータは、その音楽コンテンツデータが利用された場合の課金処理および利益分配の際に使用される。

【0024】なお、コンテンツプロバイダ200は、たとえば従来のレコード会社に相当するような、著作権を保持してコンテンツを管理している団体ごとに存在するものであり、1つのEMDシステム1に対して多数存在するものである。

#### 【0025】サービスプロバイダ250

サービスプロバイダ250は、コンテンツプロバイダ200から供給されたコンテンツプロバイダセキュアコンテナに対して、図3に示すようなサービスプロバイダセキュアコンテナを生成し、任意のデリバリチャネル300を介してユーザホームネットワーク400-1に配信する。具体的には、サービスプロバイダ250は、EMDサービスセンタ100より供給されるコンテンツプロバイダ200の公開鍵によりコンテンツプロバイダセキュアコンテナの署名検証を行う。

【0026】次に、自分が行なう配信サービスの利益分を上乗せした新たな価格情報（PT: Price Tag）を付加し、これらのデータ各々のハッシュ値をとり、サービスプロバイダ250の秘密鍵を用いて署名を生成する。この署名を、先の各データに添付してサービスプロバイダセキュアコンテナを生成し、デリバリチャネル300を介してユーザホームネットワーク400に配信する。なお、このサービスプロバイダ250も、1つのEMD

システム1に対して多数存在するものである。

#### 【0027】デリバリチャネル300

デリバリチャネル300は、任意の配信チャネルを示す。具体的には、インターネットなどの通信ネットワーク、ケーブルテレビジョンシステム、衛星放送システム、ATM通信網、移動帯通信網、パッケージメディアによる配信など、任意の配信手段を含む。

#### 【0028】ユーザホームネットワーク400

ユーザホームネットワーク400-1、400-2は、サービスプロバイダ250から配信されたサービスプロバイダセキュアコンテナを受信し、必要に応じてそのに含まれるコンテンツデータを実際使用する。ユーザホームネットワーク400の一般的な構成を図4に示す。ユーザホームネットワーク400は、各家庭ごとの音楽データの記録あるいは再生を行なう装置群であると考えるのが好適であるが、厳密には、家庭内、家庭外を問わず、任意の種々の装置により構成されるものである。より具体的には、ユーザホームネットワーク400に接続される機器としては、データ記録装置、再生装置、記録再生装置などであり、これらの各装置が、本発明に係わる装置である。

【0029】なお、以下の説明においては、説明を容易にするために、便宜上これらの機器を、通信機能を有しているネットワーク機器410と、それ自体は通信機能をもっておらず記録媒体を介して音楽データの記録および再生を行なう記録再生装置412とに分類する。すなわち、図4に示す第1のユーザホームネットワーク400-1は、2台のネットワーク機器410-1、410-2と、2台の記録再生装置412-1、412-2を有し、第2のユーザホームネットワーク400-2は、3台のネットワーク機器410-3～410-5と、4台の記録再生装置412-3～412-6を有する。そして、ネットワーク機器410の間は通信回線によるコンテンツデータの転送が可能であるが、記録再生装置412間では、記録メディア700を介してコンテンツデータが移動されることになる。

【0030】これらの各機器には、いずれも後述するSAM (Secure Application Module) チップと言われる、暗号化されたコンテンツデータの復号化および課金処理およびコピーコントロールを含む適正な権利処理を行なうためのチップが搭載されており、このチップにより適正に権利処理を行いながら音楽データの記録および再生を行なわれるようになっている。前述した、EMDサービスセンタ100からユーザホームネットワーク400に配信されるディストリビューション鍵は、各機器のこのSAMチップに格納されている。また、各ユーザホームネットワーク400には、EMDサービスセンタ100と通信可能なネットワーク機器410が少なくとも1台は設けられており、このネットワーク機器410を介して、そのユーザホームネットワーク400にお

けるコンテンツの使用履歴情報が、EMDサービスセンタ100に通報されるようになっている。

【0031】さて、このようなユーザホームネットワーク400において、いずれかのネットワーク機器410がデリバリチャネル300よりサービスプロバイダセキュアコンテナを受信すると、ネットワーク機器上のダウンロードメモリに一旦格納され、EMDサービスセンタ100より供給されるサービスプロバイダ250の公開鍵により署名検証が行なわれる。そして、各機器からの再生要求などに応じて、購入形態が決定されると、後述する使用状態情報(UCS: Usage Control Status)が生成され、SAMでディストリビューション鍵が外され、課金情報となる使用履歴情報(Usage Log)がSAMに蓄積されて、実質的にそのコンテンツが購入される。なお、蓄積された使用履歴情報は、適宜EMDシステム10に送信され、課金および決済処理に用いられる。購入されたコンテンツデータは、たとえば記録媒体などに依存したストレージ鍵により新たに鍵がかけられ、サービスプロバイダセキュアコンテナと同様に署名データが付されて、図5に示すようなユーザホームネットワークセキュアコンテナの形態で、以後、ユーザホームネットワーク400の中で流通される。

#### 【0032】セキュアコンテナ

このように、EMDシステム1においては、コンテンツデータは、図2に示したコンテンツプロバイダセキュアコンテナ、図3に示したサービスプロバイダセキュアコンテナ、そして、図5に示したユーザホームネットワークセキュアコンテナという、セキュアコンテナという形態で伝送される。各セキュアコンテナの構造については前述した通りだが、ここでは、各セキュアコンテナに含まれるUCPおよびUCSについて説明する。

#### 【0033】UCP

UCPは、コンテンツプロバイダ200によって与えられる、そのコンテンツデータの配信方針、取扱方針が記されたデータである。UCPの具体的な内容を図6に示す。図示のごとく、UCPには、そのコンテンツデータを特定するID、コンテンツプロバイダ200およびEMDサービスセンタ100の各署名データ、そのコンテンツデータの配信に係わる種々の情報、コンテンツの内容や属性に関する種々の情報、後述する利用空間調査に対する取扱制御情報、種々の課金時の条件に基づく取扱制御情報、および、そのコンテンツデータの使用形態および課金データのなどの情報が記されている。そして特に、本発明に係わる情報としては、コンテンツデータの信号諸元や圧縮方式などの情報、利用空間調査結果に対する取扱制御情報、および、各購入形態に対する取扱方針や価格情報を記録した使用制御情報が、このUCPに記録されている。

#### 【0034】UCS

UCSは、コンテンツデータを購入する際に生成される

使用状態を示すためのデータである。UCSの具体的な内容を図7に示す。図示のごとく、UCSには、コンテンツプロバイダ200、EMDサービスセンタ100およびサービスプロバイダ250の各IDおよび署名、および、その購入に関する購入者ID、決裁手段、販売価格、種々のディスカウントに係わる情報などが記されている。そして特に、本発明に係わる情報としては、後述する利用空間情報の調査結果が、このUCSに記録されている。

#### 10 【0035】ホームネットワーク機器

次に、本発明に係わる、このようなEMDシステム1のユーザホームネットワーク400において用いられる、代表的な機器についてその構成を説明する。図8は、SAMを収容する記録メディア710に対してデータの記録および再生を行なう記録再生機器414の主要部の構成を示す図である。記録再生機器414は、ホストCPU510、システムメモリ512、SAM600、フラッシュEEPROM514、ドライブCPU520、メディアSAMI/F522、EMD系メディア検出器524およびメディア検出スイッチ526を有する。

20 【0036】ホストCPU510は記録再生機器414全体を制御するCPUである。システムメモリ512は、ホストCPU510における種々の処理に用いられるメモリであり、記録メディア710が装着された際には、コンテンツファイルのファイルシステムが記録される。SAM600はコンテンツデータの権利処理および復号処理などの処理を行なうチップである。SAM600は、メディア検出スイッチ516によりホストCPU510と接続されており、ホストCPU510からはI/Oとして制御される。すなわち、I/OライトによりSAM600にタスク依頼がなされ、またI/Oリードによりタスクの結果がセンスされる。フラッシュEEPROM514は、SAM600の外付けメモリであり、記録メディア710が装着された場合には、鍵ファイルのファイルシステムが記録される。

40 【0037】ドライブCPU520は、記録メディアに対するリード/ライト全般を制御する制御部である。ドライブCPU520は、ホストCPU510と専用バスにより接続されている。メディアSAMI/F522は、記録メディア710のメディアSAM610と通信を行なうためのインターフェイスである。EMD系メディア検出器524は、記録メディア710のマニュアルスイッチの位置を検出し、記録メディア710がEMD系メディアとして用いられているのかSCMS系メディアとして用いられているのかを検出する。メディア検出スイッチ526は、記録再生機器414に記録メディア710が装着されたことを検出するスイッチである。

50 【0038】このような記録再生機器414に装着される記録メディア710は、図示のごとく、メディアSAM610を有するEMD系メディアである記録メディア



710が装着される。記録メディア710において、メディアSAM610においては、装着される記録再生機器414の正当性のチェックや、記録されているコンテンツデータに係わる権利処理などが行なわれる。また、メディアSAM610には、メディアのユニークID、ストレージ鍵、鍵ファイルのファイルシステムおよび鍵ファイルなどが記憶される。また、記録メディア710のRAM領域716には、適切でない機器のリストであるリボケーションリスト、コンテンツファイルのファイルシステムおよびコンテンツファイルが記録される。また、この記録メディア710は、SCMS系メディアとして使用するのかEMD系メディアとして使用するのかを指定するためのマニュアルスイッチ712が設けられている。

【0039】また、図9は、SAMは実装していないもののセキュアRAM領域を有する記録メディア720に対して、データの記録および再生を行なう記録再生機器416の主要部の構成を示す図である。記録再生機器416は、ホストCPU510、システムメモリ512、SAM600、フラッシュEEPROM514、ドライブCPU520およびドライブLSI528を有する。ホストCPU510、システムメモリ512、SAM600、フラッシュEEPROM514およびドライブCPU520の構成は、前述した記録再生機器414の構成と同じである。ドライブLSI528は、記録メディア720のROM領域722およびセキュアRAM領域724にアクセスをするためのドライブ回路である。

【0040】そして、このようなドライブLSI528を介して、記録メディア720のROMおよびセキュアRAM領域にメディアのユニークID、ストレージ鍵、鍵ファイルのファイルシステムおよび鍵ファイルなどを記憶することにより、メディアSAM610が実装されていなくとも、記録メディア720をEMD系メディアとして扱うことができる。また、記録メディア720では乱数生成の必要なストレージ鍵の生成は、行なえないため、ドライブLSI528は、ストレージ鍵の生成処理も行なう。

【0041】なお、このようなホームネットワーク機器には、必要に応じて、たとえば図10あるいは図11に示すような構成のSAM600、図12に示すようなAVコーデックSAM620、および、図13あるいは図14に示すような構成のドライブSAM630が搭載される。また、記録メディア710には、図15あるいは図16に示すようなメディアSAM610が搭載される。

#### 【0042】利用空間調査

##### 概要

さて、前述したようなユーザホームネットワーク400の各機器においては、全ての機器にSAMが搭載されて

おり、これにより適正に権利処理が行なわれ、コンテンツファイルがハンドリングされるものとした。しかしながら、実際の家庭には、アナログ機器や、SCMSビットによりコピーコントロールを行なうSCMS機器などが多数存在している。また記録メディアにおいても、単なるRAM領域しか形成されていない記録メディアが多数普及している。すなわち、実際には、これらの機器や記録メディアをも含めた形態で、ユーザホームネットワーク400が構成されている場合が多い。また一方で、EMDシステム1だけを見ても、これは使用できる記録メディアや使用できるコンテンツデータの信号諸元、圧縮・符号化方式などを何ら限定されるものではない。したがって、種々の信号諸元で種々の方式により圧縮符号化されたコンテンツデータが使用されている。

【0043】そのような環境の下で、たとえば図17に示すようにあるパッケージメディアのコンテンツデータを、他の記録メディアにコピーしようとした場合には、再生側の記録メディア、再生側の機器、記録側の機器そして記録側の記録メディアと、各機器、メディアの仕様を全て把握し、さらに記録されているコンテンツデータの信号諸元や圧縮符号化方式などを把握するしただでなければ、最適な条件でコピーを行なうことはできない。さらに、そのような条件を全て把握した状態でなければ、適切な権利処理を行ない適切に利益分配を行なうこともできない。

【0044】そこで、EMDシステム1においては、このようなコピーを行なう前に、利用空間調査と称して、記録側および再生側の機器、記録メディア、信号諸元、圧縮符号化方式、さらには、権利処理方式などまでをも調査し、把握するようにしている。以下、この利用空間調査の方法、および、利用空間調査を行なった上でのコンテンツデータのコピーなどの処理について説明する。

#### 【0045】利用空間調査

本実施の形態のEMDシステム1において、利用空間調査とは、各機器およびSAMにおいて、次の4つの観点から行なう。

#### 【0046】1. EMD系かSCMS系かの調査

まず第1は、処理対象のコンテンツ、ハードウェア（機器）および記録メディアが、各々、EMDシステム1に適合したEMD系のものか、EMDシステム1に適合していない従来のSCMS系のものかを調査し、これにより記録／再生をコントロールし、権利処理、コピーコントロールおよび利益分配が適切に遂行されるようにする。

【0047】ここで、コンテンツ、ハードウェアおよび記録メディアのEMD系およびSCMS系は、次のように定義する。EMD系コンテンツとは、暗号化され、鍵ファイルとともに流通されるコンテンツである。SCMS系コンテンツとは、非暗号化された状態で、SCMSビットによりコピーコントロールされる状態で流通され

るコンテンツである。EMD系ハードウェアとは、SAMが搭載されており、SAMによる権利処理が行なえる機器である。

【0048】SCMS系ハードウェアとは、SCMSビットによるコピーコントロールに対応している機器である。EMD系メディアとは、何らかの形で記録メディア上で認証機能を有するメディアであり、2つの形態がある。1つは、SAM（メディアSAM）が搭載され、これにより認証機能を実現するメディアであり、もう1つは、メディア上にセキュアRAM領域を持ち、このセキュアRAM領域を用いて外部からの処理により認証機能を実現するメディアである。SCMS系メディアとは、SCMSビットのみを有するメディアである。

【0049】そして、これまでに説明したような権利処理およびコピーコントロールを適切に行なうためには、これら各コンテンツ、ハードウェアおよび記録メディア間の記録および再生は、次表1のように規定するとが望ましい。

【0050】

【表1】

	SCMS系メディア		EMD系メディア	
	EMD系 コンテンツ	SCMS系 コンテンツ	EMD系 コンテンツ	SCMS系 コンテンツ
SCMS系ハードウェア	×	○	×	○
EMD系ハードウェア	×	○	○	○

【0051】表1の各項目について順に説明する。まず、テーブルの左上の条件、すなわち、SCMS系メディアとSCMS系ハードウェアの組み合わせに対して、暗号化コンテンツおよび鍵ファイルからなるEMD系コンテンツを記録あるいは再生する場合、この場合は、EMD系コンテンツの暗号化コンテンツをSCMS系ハードウェアでは処理できないので、仮にSCMS系メディアにEMD系コンテンツが記録されていたとしても再生できないし、新たにEMD系コンテンツを記録することもできない。

【0052】次に、左下の条件、すなわち、SCMS系メディアとEMD系ハードウェアの組み合わせに対して、EMD系コンテンツを記録あるいは再生する場合、この場合は、技術的には単に記録し再生するという処理は可能である。しかしながら、SCMS系メディアという、何ら権利処理に係わる構成、セキュアな処理に対応した構成を保持していない媒体に対してそのような処理を行なうことは、EMDシステム1の権利処理を無効にし、虚偽の処理や不正な流通を発生させる原因となるものである。したがって、SCMS系メディアへのEMD系コンテンツの記録、また、仮に記録されていたとしても、SCMS系メディアからのEMD系コンテンツの再生は、行なえないようにするのが適切である。

【0053】次に、SCMS系メディアとSCMS系ハードウェアの組み合わせに対して、SCMS系コンテンツを記録あるいは再生する場合、この場合は、従来のSCMSビットによるコピーコントロールシステムと同じ

であり、再生および記録ともそのSCMSビットに従って可能である。また、SCMS系メディアをEMD系ハードウェアに装着した場合にSCMS系コンテンツを記録あるいは再生する場合、この場合は、EMD系ハードウェアの仕様として、記録あるいは再生を行なえるようにしてもよいし、行なえないようにしてもよいが、記録メディアの上位互換性という観点において、再生および記録とも可能にしておくのが好適である。

【0054】次に、EMD系メディアとSCMS系ハードウェアの組み合わせに対してEMD系コンテンツを記録あるいは再生する場合、この場合も、前述したSCMS系メディアとSCMS系ハードウェアに対するEMD系コンテンツの記録／再生の場合と同様に、EMD系コンテンツの暗号化コンテンツをSCMS系ハードウェアでは処理できないので、記録および再生とも不可能である。次に、EMD系メディアとEMD系ハードウェアの組み合わせに対してEMD系コンテンツを記録あるいは再生する場合、この場合は、本EMDシステムの典型的な流通形態であり、EMDシステムの権利処理ルールに従って、記録および再生とも可能である。

【0055】次に、EMD系メディアとSCMS系ハードウェアの組み合わせに対して、SCMS系コンテンツを記録あるいは再生する場合、この場合は、単にEMD系メディアをSCMS系メディアとして扱えばよい訳なので、技術的にも記録／再生可能であり、また、メディアの互換性という観点からも、記録／再生可能とすべきである。また、EMD系メディアとEMD系ハード

エアの組み合わせに対してSCMS系コンテンツを記録および再生する場合、この場合も、EMD系ハードウェアにおいてEMD系メディアをSCMS系メディアとして扱えばよい訳なので、技術的にも記録／再生可能であり、また、前のケースと同様に、メディアの互換性という観点からも記録／再生可能とするべきである。

【0056】このような利用空間調査を行なうために、EMDシステム1においては、次のような構成を用いている。まず、表1に示したような記録／再生可能な条件を設定することにより、EMD系ハードウェアにおいては、EMD系メディアがセットされた場合に、そのEMD系メディアがEMD系メディアとして使用されている場合とSCMS系メディアとして使用されている場合とがあることになる。そこで、図8を参照して前述したように、EMD系メディアには、使用形態、すなわち、EMD系メディアとして使用するのかSCMS系メディアとして使用するのかを示すマニュアルスイッチ127を具備し、EMD系ハードウェアにおいては、EMD系メディア検出器524によりこれを検出するようにしている。

【0057】また、EMD系メディアに記録されているコンテンツは、EMD系ハードウェアで記録された場合には暗号化されたEMD系コンテンツとして記録され、SCMS系ハードウェアで記録された場合には暗号化されていないSCMS系コンテンツとして記録されている。すなわち、1つのEMD系メディアには、異なる形態のコンテンツが混在して記録されていることになる。したがって、再生する場合には、その記録形態を判別する必要がある。そこで、EMDシステム1においては、コンテンツの形態は各EMD系メディアのTOCに記録しておくようにしている。具体的には、TOCに、SCMS系コンテンツであれば0、EMD系コンテンツであれば1となるようなフラグを設けている。これにより、EMD系ハードウェアにおいては、TOC情報に応じてシステムを切り換えるようにすれば、適切に再生が行なえる。

#### 【0058】2. 所有権の調査

EMDシステム1においては、物理的にはコピー可能な場合であっても、権利処理の関係から、コピーを不可能にしたり、課金処理を行なう場合などがある。具体的には、コンテンツデータのコピーに関しては、コピーフリーの私的録音か課金処理を行なう個人間売買かを判別する必要がある。そこで、記録メディアおよびハードウェアの所有者を調査し、たとえば、他人のハードウェアに自分の記録メディアを搭載しているなどという状態を検出する。そして、これに基づいてコピーの制限や、課金処理を行なう。

#### 【0059】3. 権利分配のための利用空間調査

EMDシステム1においては、コンテンツデータの配信により得られた利益は、最終的にEMDサービスセンタ

100において、その配信に係わった関係者に所定の比率で分配されるようになっている。そして、その関係者としては、たとえば機器製造者や、圧縮符号化方式など特定の処理の権利者なども含まれる。したがって、権利分配の観点から、それら関係者は全て調査して把握しておく。

#### 【0060】4. フォーマット変換係数に関する利用空間調査

EMDシステム1においては、種々の信号諸元のコンテンツデータを扱っている関係上、コピーなどを行なう場合にはレート変換などの信号諸元の変換が必要となる場合がある。そして、課金処理を行なう場合には、このような変換に基づく信号の劣化などを考慮する必要がある。すなわち、品質の劣化を伴うコピーは安価にし、高い品質でコピーされる場合は高い価格を設定するのが望ましい。そこで、コピー時などに、これら信号諸元を調査しておき、課金処理時に考慮する。また、この信号諸元の変換に係わる調査は、実際に信号の変換を行なう処理の制御にも必要である。

#### 20 【0061】利用空間調査手順

そして、たとえば図17に示したようなコピーを行なう場合には、次のような手順で利用空間調査を行なう。まず、再生側において、メディアとハードウェア間の利用空間の調査を行なう。そのため、まず再生側の記録メディアのメディアSAMが再生機器に対して自分の素性を送る。次に、再生機器においては、SAMに利用空間ディスクリプタを生成し、再生側の機器のSAMに記述されているその機器の扱える信号処理などの利用空間のデータを、利用空間ディスクリプタにセットする。

30 【0062】次に、その利用空間ディスクリプタに、メディアの情報をセットする。すなわち、メディアとハードウェアの間で相互認証を行なって、両サイドでセッション鍵を保有し、メディアSAMの中に記述されているセキュアデータを全て、ハードウェアのSAMに転送する。これにより、再生側の利用空間調査は終了する。次に、記録側においても、記録機器と記録メディアの間で、同様の利用空間調査を行なう。そして、最後に、記録機側の利用空間調査結果を再生側に送ることにより、再生側の機器のSAMに、利用空間ディスクリプタが完成する。このようにして生成される利用空間ディスクリプタ（利用空間テーブルとも言う。）を図18に示す。

【0063】なお、ここでは再生側と記録側が1対1の場合を示したが、再生側1に対して、複数の記録機器に対してコピーを行なう場合もある。このような場合には、各々図18に示したのと同様の情報で構成される、図19に示すような、利用空間調査テーブルを生成する。

#### 【0064】ホームネットワーク機器の動作

次に、前述したような本発明に係わるユーザホームネットワーク400の各機器において、たとえば図17に示

したようなパッケージメディアからパッケージメディアへ音楽データを複写する際の前述した利用空間調査の処理を含む動作について、図20～図27のフローチャートを参照して説明する。なお、実際にコンテンツデータのコピーを開始した以降は、既存の通常の機器の処理と同じであるので、ここでは、実際のコピー動作以前の初期動作を中心に説明する。

【0065】まず、この初期動作の処理の全体の流れについて、図20のフローチャートを参照して説明する。まず最初に、搭載された記録媒体の種別判別を行い（ステップS11）、搭載されている記録媒体がEMD系メディアであった場合には（ステップS12）、さらにそのメディアがSAMを有し自らストレージ鍵を生成することのできるアクティブなメディアであるか否かを検査する（ステップS13）。記録メディアが、SAMを有していないメディアであった場合には、ドライブLSI528でストレージ鍵を生成しておく（ステップS14）。

【0066】次に、記録メディアがアクティブメディアの場合には公開鍵方式により、また、記録メディアがポジティブメディアの場合には共通鍵方式により、記録メディアとドライブCPU520との間で相互認証を行なう（ステップS15）。（以後の説明は、記録メディアがアクティブメディア710であるとして説明を行なう。）

次に、記録メディアに記録されているリヴォケーションリストを更新する処理を行い（ステップS16）、更新が終了したら、まずメディアSAM610からSAM600の対してのリヴォケーションチェックを行い、次にSAM600～メディアSAM610へのリヴォケーションチェックを行なう（ステップS17）。

【0067】そして、鍵データブロックの物理アドレス情報のSAMへの転送および設置処理を行い（ステップS18）、さらに、鍵データブロックのSAM600およびAV圧縮伸張部への転送処理を行い（ステップS19）、最後にファイルシステムをシステムメモリ512に転送する処理を行い（ステップS20）、利用空間調査を含む、コンテンツデータの転送以前の一連の初期処理を終了する（ステップS21）。以後、各処理について詳細に説明する。

【0068】まず、ステップS11の、記録メディアの種別判別の処理について図22のフローチャートを参照して説明する。まず、たとえばメディア検出スイッチ526が記録メディア710の挿入を見地するなどして処理を開始したら（ステップS30）、メディア検出スイッチ526はこれをドライブCPU520に通知する（ステップS31）。また、EMD系メディア検出器524においては、記録メディア710のマニュアルスイッチ712に状態が検出され（ステップS32）、記録メディア710の判別結果がドライブCPU520に通

知される（ステップS33）。

【0069】そして、記録メディア710がEMD系メディアであった場合には（ステップS34）、ドライブCPU520が、メディアSAMI/F522を介して記録メディア710のメディアSAM610に対して、乱数生成を要求する（ステップS35）。これにより、もし記録メディア710がメディアSAM610を有するアクティブな記録メディアであった場合には、メディアSAM610で乱数が生成され（ステップS67）、生成した乱数がメディアSAMI/F522を介してレジスタに格納され（ステップS37）、メディアSAMI/F522からドライブCPU520に乱数が格納された旨が通知される（ステップS38）。すなわち、これらの動作の有無により、ドライブCPU520は記録メディアがアクティブメディアかポジティブメディアかを判別することができる（ステップS39）。

【0070】そして、ドライブCPU520がホストCPU510に、搭載して記録メディアの種別を通知し（ステップS40）、同時にSAM600も、記録メディアの種別情報をスタックし（ステップS41）、記録メディアの種別判別処理が終了する（ステップS42）。

【0071】次に、ステップS15の、相互認証処理について、図22のフローチャートを参照して説明する。まず、処理がスタートしたら（ステップS90）、ホストCPU510が、SAM600に対して、記録メディア710と相互認証を行なうようにファンクションコールを送る（ステップS91）。これに基づいて、メディアSAM610とSAM600との間で、公開鍵暗号をベースとした相互認証を行なう（ステップS92）。そして、SAM600はSAM600に対して結果を通知し（ステップS93）、相互認証処理は終了する（ステップS94）。

【0072】次に、ステップS16の、リヴォケーションリストの更新処理について図23のフローチャートを参照して説明する。まず、処理が開始されたら（ステップS50）、メディアSAM610に格納されているリヴォケーションリストをストレージ鍵で復号する（ステップS51）。次に、そのリヴォケーションリストを、SAM600の公開鍵で暗号化し（ステップS52）、メディアSAMI/F522、ドライブCPU520およびホストCPU510を介して、SAM600に転送してもらう（ステップS53）。転送された、リヴォケーションリストは、SAM600内で、SAM600の秘密鍵を用いて復号化される（ステップS54）。

【0073】そして、SAM600に格納されているリヴォケーションリストを読み出し（ステップS55）、MAC鍵で復号してSAM600内部に格納されているMAC値と比較し、改ざんがないことをチェックする（ステップS56）。そして、記録メディア710から

読み出したリヴォケーションリストと、SAM600に格納していたリヴォケーションリストのバージョン番号を比較し（ステップS57）、SAM600に格納していたリヴォケーションリストの方が新しければ（ステップS58）、このリヴォケーションリストをメディアSAM610の公開鍵で暗号化し（ステップS59）、ホストCPU510、ドライブCPU520およびメディアSAMI/F522を経由してメディアSAM610に転送することにより（ステップS60）、メディアSAM610のリヴォケーションリストを更新し、処理を終了する（ステップS61）。

【0074】次に、ステップS17の、リヴォケーションリストのチェックの処理について、図24のフローチャートを参照して説明する。まず、チェックの処理が開始されたら（ステップS71）、メディアSAM610からSAM600にコマンドを送ることにより（ステップS72）、SAM600のIDがメディアSAM610に転送される（ステップS73）。メディアSAM610は、このIDがリヴォケーションリストに含まれているか否かをチェックし、含まれていた場合には、このSAM600を有する機器は、たとえば何らかの不正を行なうなど不適切な装置であると判定され、メディアSAM610は記録再生機器414との通信を拒絶し（ステップS76）、処理を終了する（ステップS77）。

【0075】SAM600のIDがリヴォケーションリストに含まれていない場合には（ステップS75）、次にSAM600からメディアSAM610のチェックが開始され（ステップS78）、SAM600からメディアSAM610にコマンドが送られて（ステップS79）、メディアSAM610のIDがSAM600に転送される（ステップS80）。SAM600は、このIDがリヴォケーションリストに含まれているか否かをチェックし、含まれていた場合には、この記録メディア710はたとえば何らかの不正が行なわれたなど不適切な記録メディア710であると判断し、以後の通信を拒絶し（ステップS83）、処理を終了する。メディアSAM610のIDがリヴォケーションリストに含まれていない場合には（ステップS82）、SAM600およびメディアSAM610とも適正なSAM、すなわち、記録再生機器414および記録メディア710はともに適正な装置および媒体であると判断され、一連のチェック処理は終了する（ステップS85）。

【0076】次に、ステップS18の、鍵データブロックの物理アドレス情報の上位への転送処理について、図25のフローチャートを参照して説明する。まず、処理がスタートすると（ステップS100）、鍵データブロックの物理アドレスの情報をストレージ鍵で復号し（ステップS101）、鍵データブロックの物理アドレス情報をメディアSAM610の公開鍵で暗号化する（ステップS102）。そして、メディアSAM610は、こ

の暗号化された情報を、メディアSAMI/F522、ドライブCPU520およびホストCPU510を介して、SAM600に転送する（ステップS103）。

【0077】SAM600では、鍵データブロックの物理アドレス情報全体のハッシュ値を取り、データ全体が改ざんされていないかどうかのチェックを行い（ステップS104）、適正であればその物理アドレス情報をSAM600内にセットする（ステップS105）。次に、AVコーデックSAM620と共通鍵暗号をベースとした相互認証を行い（ステップS106）、セッション鍵を共有し（ステップS107）、鍵データブロック情報をAVコーデックSAM620に転送する（ステップS108）。AVコーデックSAM620では、これをセッション鍵を用いて復号し（ステップS109）、鍵データをメモリに格納し（ステップS110）、一連の転送処理は終了する（ステップS111）。

【0078】次に、ステップS19の、鍵データブロックの上位への転送処理について、図26のフローチャートを参照して説明する。まず、処理がスタートすると（ステップS120）、鍵データブロックをストレージ鍵で復号し（ステップS121）、鍵データブロックをメディアSAM610の公開鍵で暗号化する（ステップS122）。そして、メディアSAM610は、この暗号化された情報を、メディアSAMI/F522、ドライブCPU520およびホストCPU510を介して、SAM600に転送する（ステップS123）。

【0079】SAM600では、鍵データブロック全体のハッシュ値を取り、データ全体が改ざんされていないかどうかのチェックを行う（ステップS124）。そして、適正であれば、AVコーデックSAM620と共通鍵暗号をベースとした相互認証を行い（ステップS125）、セッション鍵を共有し（ステップS126）、鍵データブロックをAVコーデックSAM620に転送する（ステップS127）。AVコーデックSAM620では、これをセッション鍵を用いて復号し（ステップS128）、鍵データをメモリに格納し（ステップS129）、一連の転送処理は終了する（ステップS130）。

【0080】そして最後に、ステップS20で示した、ファイルシステムの上位への転送処理について、図27のフローチャートを参照して説明する。まず、処理がスタートすると（ステップS140）、ドライブCPU520が記録メディア710上の物理アドレス情報を管理するコンテンツファイルのファイルシステムを検出して、記録メディア710より読み出す（ステップS141）。次に、ドライブCPU520は、このファイルシステムをホストCPU510に転送し（ステップS142）、ホストCPU510は、これをシステムメモリ512上に記憶し（ステップS143）、ファイルシステムの転送処理は終了する（ステップS144）。

## 【0081】EMDシステム1の動作

最後に、このような利用空間調査を行なう前述したような構成のEMDシステムにおける、音楽コンテンツの配信の動作、処理の流れについてまとめて説明する。

## 【0082】情報配信

まず、音楽コンテンツデータの配信処理の流れについて、典型的な一例を挙げて今一度まとめて説明する。まず、図1に示すようなEMDシステム1において、コンテンツプロバイダ200で著作権者により管理されている音楽コンテンツデータは、図2に示したコンテンツプロバイダセキュアコンテナの形態でサービスプロバイダ250に供給される。サービスプロバイダ250は、その音楽コンテンツデータを、図3に示したサービスプロバイダセキュアコンテナの形態で、種々のサービス形態により、また種々のデリバリチャネル300を介して、たとえば図4に示すような構成のユーザホームネットワーク400に配信する。この際、いわゆるポータルといわれる業者などにより、そのコンテンツデータの一部が使用されて、音楽コンテンツの参照、紹介、批評あるいは新たな形態の間接的な販促活動などが行なわれる場合もある。

【0083】このようにしてユーザホームネットワーク400に配信された音楽コンテンツデータは、配信された直後は、通常は特段の処理が行なわれずに、サービスプロバイダセキュアコンテナの形態でそのまま家庭内のストレージ機器のハードディスクなどに記憶される。そして、使用者がこのサービスプロバイダセキュアコンテナに含まれる音楽データを再生したり記録する、すなわち使用すると決定し、たとえば家庭内の記録再生装置412において相応の操作を行った場合に、記録再生装置412内のSAMが、サービスプロバイダセキュアコンテナ内の図6に示したようなUCPを読み出し、UCP内に設定されている取扱方針で許される範囲内での使用形態を決定し、使用状態を示すUCSを生成し、図5に示すようなユーザホームネットワークセキュアコンテナが生成される。

【0084】以後、家庭内の記録再生装置412において、EMDサービスセンタ100より予め配布されているディストリビューション鍵を用いることにより、暗号化された音楽コンテンツデータが適宜復号されて再生されるなど使用される。また、このユーザホームネットワークセキュアコンテナの形態で、許される範囲内で順次コピーが行われる。

## 【0085】ホームネットワーク機器の動作

ユーザホームネットワーク400の各ホームネットワーク機器間におけるデータの流れ、および、データ配信状態について図28～図42の各具体例を参照して説明する。

【0086】まず、図28に、機器のホストCPU500とSAM600およびメディア710との関係を示

す。前述したように、SAM600は、ホストに対してI/Oとして接続されており、I/O命令により制御される。ホストCPU500に対しては、SAM600はスレーブ、SAM600とメディア710の間では、SAMがマスタ、メディアがスレーブとなる。メディア710はSAM600に接続されており、ファンクションコールおよびリザルトにより処理を進める。ファンクションコールはコマンドとコンテンツを特定するための番号を含む情報である。キーファイルは、メディアとSAMとで処理し、コンテンツファイルは、SAMが処理する場合もあるし、ホストCPUが記録する場合もある。ファイルシステムは、キーファイルのファイルシステムはSAMに展開し、コンテンツファイルのファイルシステムはホストCPUに展開する。

【0087】図29は、AVコーデックを有する機器における、ホストCPU、SAM、AVコーデックSAMおよびメディアとの関係を示す図である。この形態の機器では、メディアを挿入した時点で、キーファイルはまとめてSAMに展開し、新たに加わったキーデータも含めて、イジェクト時にまとめてメディアに転送する。この場合は、メディアSAMとSAMとの間で、公開鍵方式により相互認証を行なってセッションキーを生成し、セッションを行なって、キーファイルとキーファイルTOCとをSAM側にストックする。

【0088】コンテンツファイルは、ホストCPU側にファイルシステムを送る。これによりホストCPUがファイルシステムを読んで、特定のコンテンツファイルをコーデックSAMに送るように命令すると、SAMとAVコーデックSAMとがトリプルDESによる相互認証を行なってセッションキーを生成し、これにより所望のコンテンツ、たとえば、コンテンツ1、4、5のコンテンツキーをSAMからAVコーデックSAMに転送する。また、アナログ出力のためのウォーターマークデータも、セッションキーにより暗号化してAVコーデックSAMに転送する。これにより、メディアから再生した圧縮データを、AVコーデックSAMでリアルタイムに復号化し、ウォーターマークを付加して出力する。

【0089】図30は、ハードディスクに暗号化されたコンテンツファイルがCAを介して、ダウンロードされてきて、これを試聴してみて、再生してみて、利用形態を決定するというプロセスを説明するための図である。この装置においては、コンディショナルアクセス(CA)が、デリバリーサービスより、たとえばCF-1～CF-20の20個のコンテンツファイルをダウンロードしてくる。そして、コンテンツファイルはAV-ハードディスク530に、キーファイルは、SAMにより管理されるEEPROM514にロードされる。SAMとAVコーデックSAMでトリプルDESで相互認証を行い、再生したいコンテンツのキーファイルをAVコーデックSAMに送り、AVコーデックで再生出力する。

【0090】ホストCPUは、SAMに対してI/Oリードライトでファンクションコールを送ってリザルトをもらう。また、HDDに対してもI/Oリードライトで指令をして、たとえばコンテンツ7を読み出しAVコーデックに出力させる。SAMは、メモリリードライトによりファイルシステムに基づいて、ファイルシステムをスタックして、コンテンツキーAVコーデックに送る。GUIでボタンを押された、ホストに割り込みが入って、ダウンロードが開始される。ダウンロードが開始されたら、ホストはSAMにお願いし、キーファイルを格納させる。

【0091】図31は、ハードディスクの中にセキュア領域がある場合である。この場合は、ハードディスクの中にキーファイルを入れてしまい、HDDは、ホストとSAMの共有記憶空間になる。HDDに記憶されているキーファイルにはSAMのみがアクセス可能である。鍵ファイルのファイルシステムはサムがスタックし、コンテンツファイルのファイルシステムは、ホストCPUがスタックする。

【0092】図32は、ネットワーク機器の中にパッケージメディアが入っている場合の構成を示す。この場合は、サムとメディアSAMが相互認証を行い、キーファイルをセッションキーでメディアSAMに送る。そして、メディアSAM側で、セッションキーを解いて、ストレージキにより暗号化し、鍵のかけかえを行ない、メディアSAMに記録する。サムは、ホストにOKを返答し、ホストはI/Oリードライトで、コンテンツファイルをメディアに記録する。この時に、利用空間を調査し、必要であれば、諸元変換を行ってから記録する。

【0093】図33は、図17に示したのと同様の、EMDシステム1における典型的な複写処理の例である。この構成では、ネットワーク機器と別にパッケージ機器があって、物理的な線でつないでダウンロードする。したがって、SAM-SAM間の認証が必要となる。認証は、両機器のホストとSAM間と、SAM-SAM間で行なわれる。再生側は、キーファイルをメモリから取り出して、SAM-SAM間で相互認証を行いセッションキーをつかって、キーファイルを記録側に送る。記録側では、メディアSAMと相互認証を行なってメディアのキーファイルを展開する。

【0094】購入形態は、送り側で決めてもよいし、記録側で決めてもよい。利用空間調査は、両サイドの機器で行なう。再生側のホストCPUが持っているのはハードディスクに記録されているコンテンツファイルのファイルシステムであり、SAMの持っているキーファイルのファイルシステムは、メモリに記録されているキーファイルのファイルシステムである。記録側のホストCPUが持っているのはパッケージメディアに記録されているコンテンツファイルのファイルシステムであり、SAMに持っているキーファイルおよびファイルシステム

は、パッケージメディアのものである。

【0095】図34は、パッケージ間の再配付の場合を示す図である。再生の機器とメディアで利用空間調査を行い、SAMと記録系でメディア空間を行い、キーファイルはSAMに展開して、コンテンツファイルはHDD上に展開する。利用形態は、UCPを移すのみ。したがって、セッションキーをつかって、UCP、キーファイルのみを転送し、コンテンツファイルはそのまま転送する。SAMとメディアSAMで相互認証し、キーファイルを送り、コンテンツファイルはメディアに記録する。再生側でUCSを作り、購入形態を決める。記録側に転送する時は、KF1-UCPだが、メディアに記録される時には、KF1-UCP/UCSとなっている。なおこの場合、利用空間調査で諸元が同じことがわかって

いるものとする。

【0096】図35は、諸元が違う場合の例である。再配付だけど諸元が違う。この利用空間では、再生側に変換処理を持っているので、コンテンツはコンテンツキーで復号し、コンテンツキーを記録側にセッションキーで送る。そして、信号を変換して、セッションキーで送って、記録側にスタックしているコンテンツキーで再暗号化してメディアに記録する。再暗号化はドライブで行なう。ドライブにDESがあるので、ここで暗号化しながら記録する。

【0097】図36は、UCSからの購入の例を示す図である。再生課金の場合を示し、利用空間調査と、キーファイル展開の操作は前述した場合と同じである。この場合、諸元は同じであり、セッションキーは、SAM-SAM間、SAM-メディアSAM間で持っている。また、UCSのキーファイルをセッションキーで送る。

【0098】図37は、買い切りの場合である。利用空間調査の中に、誰が購入したか。また、記録媒体は誰のものという判別により、私的録音、プライベートユーザー/セルの区別をつける。所有権の利用空間調査も必要である。UCSに記録されている所有者から、その記録媒体の所有者が同じなら移る。そうでない場合は課金される。

【0099】図38は、EMDからSCMSコンテンツへのコピーを示す。利用空間調査で相手がSCMSとわかるので、SAMで課金を行い、コンテンツキーで暗号化をはずしながら、1394コピープロテクションのセッションキーを使って、ホスCPU2に送って、メディアに記録する。この時のプロテクトモードは、コピー付加である。

【0100】図39は、利用空間調査でSAM機器にSCMS機器が乗っている場合である。EMD機器同志のセッションであるが、記憶側に載っているメディアがSCMSメディアなので、UCPに書かれているEMDモードと諸元、および、相手の記録媒体のSCMSということで処理を行なう。この場合は、UCPに書かれてい

るSCMSメディアへの記録という報告を見て、1回当たりのコピーの価格をみて、これを再生側のEMD機器で支払う。再生側でコンテンツ鍵ではずして、セッション鍵で転送して記録してもいいが、記録側で記録するようにしてもよい。

【0101】図40は、再生側がSAM機器で、SAMメディアだが、マニュアルスイッチによりSCMSメディアとして使用され、SCMSコンテンツが搭載されている場合である。この例では、SAM機器で、EMDメディアでEMDモードで使用している機器にコピーを行なう。この場合、TOC情報によりSCMSコンテンツであることがわかっているので、SCMSコンテンツとして処理を行なう。送る時は、SAM-SAMで相互認証して、セッションキーを作って、SCMSコンテンツは、セッション鍵で暗号化して記録側に送り、記録側ではセッション鍵を用いてはずす。そして、記録側で、コンテンツ鍵を生成して、これで暗号化して、メディアに記録する。最後に、生成したコンテンツキーをメディアSAMに送って、セッション鍵をストレージ鍵で鍵をかけるおし保存する。

【0102】図41は、シングルドライブコピーを示す。この場合、まず、ROMを入れ、キーファイルはSAM1に転送しファイルシステムを展開する。コンテンツファイルは、共有メモリ空間におく。次に、ROMディスクをはずす。RAMディスクをセットする。そして、SAM1で購入形態処理を決定した上で、決定した鍵ファイル(UCS鍵ファイル)および、商品そのもののUCP鍵ファイルをRAMのメディアSAMに記録する。最後に、コンテンツをRAMに記録する。このようにすれば、デッキは2台必要なく、シングルのデッキでコピーできる。

【0103】図42は、ROMディスクでの購入形態を示す。ROMを買った時は、購入形態がきまっていない。また、ROM-RAMのハイブリッドが必要となる。この場合、メディアSAMにあるキーファイルを全部SAM1に転送し、試聴して、購入するコンテンツを選択する。そして、UCSキーファイルを作り、メディアSAMに記録する。これにより、買った曲だけが聞けるROMディスクになる。RAMは、セキュアRAMのみの場合、セキュアRAMとメディアSAMがある場合、セキュアRAMがなくて全部メディアSAMでやってしまう場合がある。

#### 【0104】使用履歴情報

そして、このような種々の形態により、音楽コンテンツが課金される形態で実際に使用されるごとに、使用履歴情報(Usage-Log)が生成される。生成された使用履歴情報(Usage-Log)は、各ユーザホームネットワーク400内のネットワーク機器410に一旦蓄積された後、適宜EMDサービスセンタ100に送信される。

【0105】この使用履歴情報(Usage-Log)の一例を図

43に示す。使用履歴情報(Usage-Log)には、図43に示すように、コンテンツID(Content ID)、コンテンツを使用した利用者ID(User ID)、ユーザホームネットワーク400を特定するホームネットワークグループID(Home Network Group ID)、権利処理を行なったSAMのID(SAM ID)、購入形態を示す情報(Purchase/Usage mode)、価格(Price Tag)、使用地域(area-code)、割引情報(discount information)、そのコンテンツの販売に係わった全てのエンティティのID、使用の際の信号諸元の情報などが記録されている。エンティティとしては、コンテンツプロバイダ(Content Provider)、サービスプロバイダ(Service Provider)を初めとして、ポータル(E.M.Place)、ハードウェア提供元(H/W Provider)、記録媒体提供元(Media Provider)、装置製造元(Component Provider)、権利者(LicenceHolders)など、そのコンテンツの配信に係わった全てのエンティティが記録される。

#### 【0106】利益分配処理

さて、このようなEMDシステム1、またユーザホームネットワーク400における音楽コンテンツデータの配信環境において、最終的に音楽コンテンツデータの購入に基づく利益を分配する方法について図44~図46を参照して説明する。なお、ここで言う利益とは、音楽コンテンツの配信に伴って得られる金銭的な価値を広く総称したものであって、実際の適用時には、購入金額、対価をそのまま用いてよい。図44は、利益分配処理の流れを示すブロック図であり、図45は、図44に示した利益分配率データを説明するための図であり、図46は、図44に示した利益分配処理を説明するための図である。

【0107】前述したように、まず、EMDサービスセンタ100には、図44に示すように、基本的にEMDシステム1の全てのエンティティが登録されており、ID、種々の属性、決済口座などの情報を含むエンティティ管理データ110が記録されている。また、図45に示すような、各コンテンツプロバイダ200から登録された、各コンテンツIDごと、すなわち、コンテンツプロバイダセキュアコンテナごとの、各エンティティに対する利益分配の割合を示した利益分配率データ112が記録されている。さらに、図示しないが、各コンテンツプロバイダ200から登録された、各コンテンツデータの配信の際の信号諸元に基づいた価格変更、価格換算を規定した価格換算データ114が記録されている。

【0108】このような状況において、音楽コンテンツデータが購入されたら、前述したような各機器のSAMあるいはメディアSAMにおけるセキュアな処理により利用空間調査が行なわれ、最終的に、コンテンツの生成から購入に関わった全てのエンティティ、購入条件、信号諸元などが記録された、図43に示したような使用履歴情報(Usage-Log)がEMDサービスセンタ100に送



信されてくる。

【0109】この使用履歴情報(Usage-Log)を、EMDサービスセンタ100のたとえば利益分配サーバ120が受信したら、まず、最終的な購入価格を決定する。購入価格は、まず基本的に、買い切り(Sell Through)の場合は使用履歴情報(Usage-Log)に記載されているプライスタグが基準となり、また再生課金(Pay PerPlay)による購入の場合には1回の再生価格×使用履歴情報(Usage-Log)の個数が基準となる。そして、この基準価格に、さらに種々の条件に基づいて補正を行ない、最終的な購入価格を決定する。

【0110】具体的には、まず、使用履歴情報(Usage-Log)に記載されている購入時の信号諸元のデータに基づいて、価格換算データ114を参照して換算を行なう。たとえば、プライスタグが1ビット2、28224MHzのサンプリングデータを基準としたものである場合に、これを16ビット44、1KHzATRAC(登録商標)2にダウンサンプリングして購入した場合には、価格換算データ114を参照して、品質相応の換算を行なう。次に、使用履歴情報(Usage-Log)の使用地域の情報に基づいて、使用した国に応じて異なるたとえば付加金などの価格を検出し、この調整を行なう。さらに、たとえばマイルージなどのディスカウントを利用しているか否かなどの条件を加味し、最終的な価格を決定する。

【0111】一方で利益分配サーバ120は、使用履歴情報(Usage-Log)に記載されているコンテンツIDに基づいて、コンテンツデータごとの利益分配率データ112を参照し、そのコンテンツに関わる各エンティティに対する利益の分配率を決定する。また、使用履歴情報

(Usage-Log)に記載されている各エンティティのIDに基づいて、エンティティ管理データ110を参照して、利益振込口座の口座番号を検出する。最後に、たとえば著作権利者にのみ付加される著作権料(copyright fee)のような料金の調整を行い、最終的に各エンティティに支払う価格を決定する。

【0112】支払い価格が決定されたら、たとえばEMDサービスセンタ100内の支払いサーバ130にそのデータを転送し、支払いサーバ130が、たとえば特定の期間ごとの決済処理を一括するなどした上で、カード会社や銀行などの決済機関800を介して支払い処理を行なう。

【0113】このようにすることで、コンテンツデータを配信した、あるいは使用されたことによる対価を、必要に応じて媒体メーカや装置メーカも含めた、そのコンテンツデータの配信に関わった全てのエンティティに対して、そもそもコンテンツデータを生成したコンテンツプロバイダ200が意図し設定した分配比率に従って、また、コンテンツデータの品質、購入形態、使用環境による制約などにも適切に対応した形態で、適切に配分することができる。

#### 【0114】変形例

なお、本発明は本実施の形態に限られるものではなく、任意好適な種々の改変が可能である。たとえば、本実施の形態においては音楽データの配信システムを例示したが、静止画像データ、動画像(映像)データ、ビデオデータ、あるいは、コンピュータプログラムやゲームプログラム、ゲームの追加データなど、任意のデータの配信システムに適用可能である。

【0115】また、本実施の形態においては図1に示したような構成のEMDシステム1を例示して本発明を説明したが、このような構成のシステムにのみ適用可能なものではない。たとえば、EMDサービスセンタ100が存在せず、コンテンツプロバイダ200自身が、エンティティ管理データ110、利益分配率データ112および価格換算データ114などを管理しておき、使用履歴情報(Usage-Log)を受け付けて、対価配分処理を行なうようにしてもよい。もちろん、これがサービスプロバイダ250や、EMDサービスセンタ100とは異なる第3の機関により行なわれるような構成でもよい。また、コンテンツデータの配信環境についても、任意の構成でよい。たとえば、サービスプロバイダ250が存在せずコンテンツプロバイダ200が直接に配信する構成であってもよい。

【0116】また、EMDサービスセンタ100、コンテンツプロバイダ200、サービスプロバイダ250、デリバリチャネル300、ユーザホームネットワーク400の各構成は何ら限定されるものではなく、各々任意の構成でよい。

#### 【0117】

【発明の効果】このように、本発明によれば、適切に権利処理を行いながら記録することのできるデータ記録装置を提供することができる。また記録された所望のデータを、適切に権利処理を行いながら再生することのできるデータ再生装置を提供することができる。また、所望のデータを、任意の信号諸元で任意の媒体、通信路、機器を介して任意の配信先に所定の権利処理を行いながら配信するためのデータ処理装置を提供することができる。さらに所望のデータを、適切に権利処理を行いながら記録および再生することのできるデータ記録媒体を提供することができる。

#### 【図面の簡単な説明】

【図1】図1は、本発明の一実施の形態のEMDシステムの構成を示すブロック図である。

【図2】図2は、図1に示したEMDシステムのコンテンツプロバイダが生成するコンテンツプロバイダセキュアコンテナを説明するための図である。

【図3】図3は、図1に示したEMDシステムのサービスプロバイダが生成するサービスプロバイダセキュアコンテナを説明するための図である。

【図4】図4は、図1に示したEMDシステムのユーザ

ホームネットワークの一般的な構成を示す図である。

【図5】図5は、図1に示したEMDシステムのユーザホームネットワーク内で生成するユーザホームネットワークセキュアコンテナを説明するための図である。

【図6】図6は、UCPを説明するための図である。

【図7】図7は、UCSを説明するための図である。

【図8】図8は、ホームネットワーク機器の構成の第1の例を示す図である。

【図9】図9は、ホームネットワーク機器の構成の第2の例を示す図である。

【図10】図10は、SAMの構成の第1の例を示す図である。

【図11】図11は、SAMの構成の第2の例を示す図である。

【図12】図12は、AVコーデックSAMの構成を示す図である。

【図13】図13は、ドライブSAMの構成の第1の例を示す図である。

【図14】図14は、ドライブSAMの構成の第2の例を示す図である。

【図15】図15は、メディアSAMの構成の第1の例を示す図である。

【図16】図16は、メディアSAMの構成の第2の例を示す図である。

【図17】図17は、利用空間調査の概念を説明する図である。

【図18】図18は、利用空間ディスクリプタ（利用空間テーブル）を説明するための図である。

【図19】図19は、1つの再生装置から複数の記録装置にコピーを行なう場合の利用空間調査を説明するための、利用空間調査テーブルを示す図である。

【図20】図20は、利用空間調査を含む一連の初期処理の流れを示すフローチャートである。

【図21】図21は、装着された記録メディアの種別判別処理の流れを示すフローチャートである。

【図22】図22は、相互認証処理の流れを示すフローチャートである。

【図23】図23は、リヴォケーションリスト更新処理の流れを示すフローチャートである。

【図24】図24は、リヴォケーションリストチェック処理の流れを示すフローチャートである。

【図25】図25は、鍵データブロックの物理アドレス情報の上位への転送処理の流れを示すフローチャートである。

【図26】図26は、鍵データブロックの上位への転送処理の流れを示すフローチャートである。

【図27】図27は、ファイルシステムの上位への転送処理の流れを示すフローチャートである。

【図28】図28に、ホームネットワーク機器のホストCPUとSAMおよびメディアの基本的構成を示す図で

ある。

【図29】図29は、AVコーデックを有する機器における、ホストCPU、SAM、AVコーデックSAMおよびメディアとの関係を示す図である。

【図30】図30は、ハードディスクに暗号化されたコンテンツファイルをダウンロードし、試聴した上で利用形態を決定するという状態を示す図である。

【図31】図31は、ハードディスクの中にセキュア領域がある場合を示す図である。

10 【図32】図32は、ネットワーク機器の中にパッケージメディアが入っている場合を示す図である。

【図33】図33は、EMDシステムと同様の構成による複写処理を示す図である。

【図34】図34は、パッケージ間の再配付の場合を示す図である。

【図35】図35は、諸元が違う場合の再送付の例を示す図である。

【図36】図36は、UCSからの購入の例を示す図である。

20 【図37】図37は、買い切りの場合を示す図である。

【図38】図38は、EMDからSCMSコンテンツへのコピーを示す図である。

【図39】図39は、利用空間調査でSAM機器にSCMS機器が乗っている場合を示す図である。

【図40】図40は、再生側がSAM機器でSAMメディアだが、マニュアルスイッチによりSCMSメディアとして用いられている場合を示す図である。

【図41】図41は、シングルドライブコピーを示す図である。

30 【図42】図42は、ROMディスクでの購入形態を示す図である。

【図43】図43は、利用履歴情報（Usage-Log）の内容を説明するための図である。

【図44】図44は、図1に示したEMDシステムにおける利益分配処理の流れを示すブロック図である。

【図45】図45は、図44に示した利益分配率データを説明するための図である。

【図46】図46は、図44に示した利益分配処理を説明するための図である。

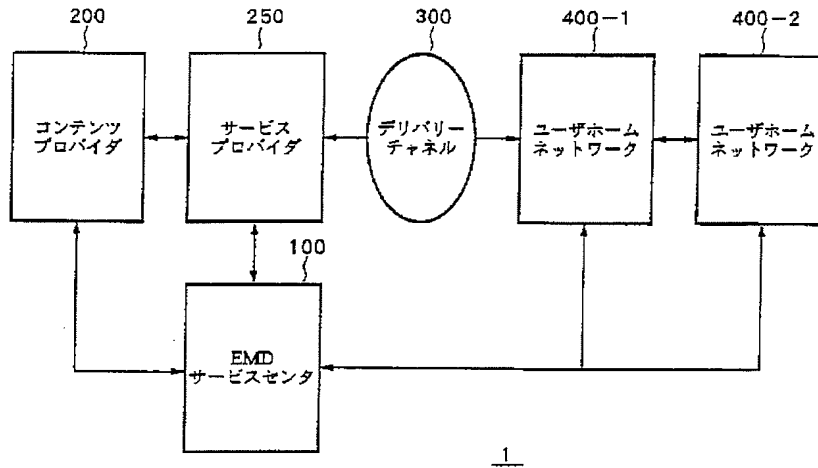
40 【符号の説明】

1…EMDシステム、100…EMDサービスセンタ、110…エンティティ管理データ、112…利益分配率データ、114…価格換算データ、120…利益分配サーバ、130…支払いサーバ、200…コンテンツプロバイダ、250…サービスプロバイダ、300…デリバリチャネル、400…ユーザホームネットワーク、410…ネットワーク機器、412、414、416…記録再生機器、500…ホストCPU、512…システムメモリ、514…フラッシュEEPROM、516…ホストCPUバス、520…ドライブCPU、522…メデ

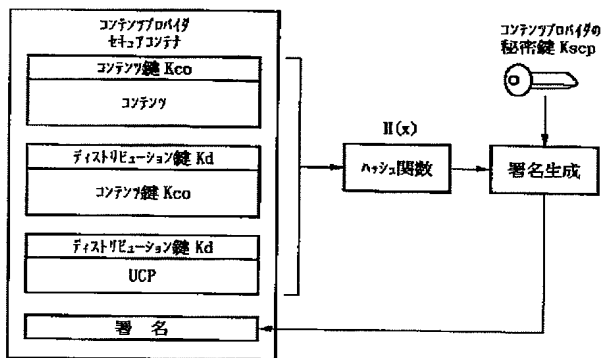
33

ィアSAMインターフェイス、524…EMD系メディア検出器、526…メディア検出スイッチ、600…SAM、610…メディアSAM、620…AVコーデックSAM、630…ドライブSAM、700…記録媒

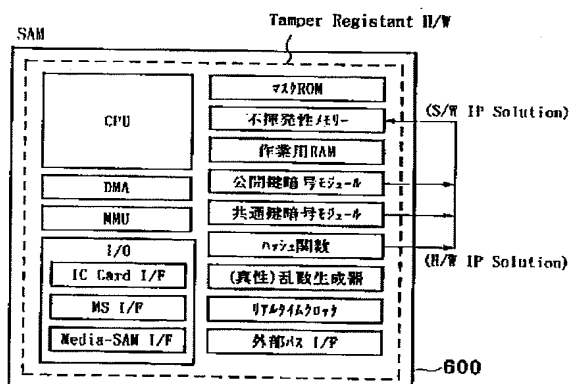
【図1】



【図2】



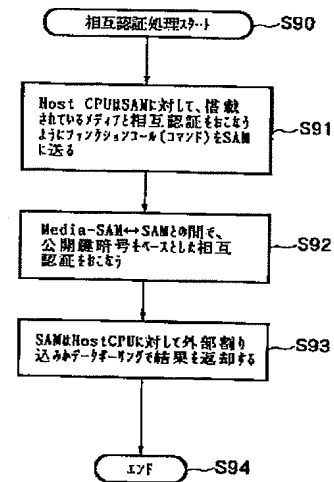
【図10】



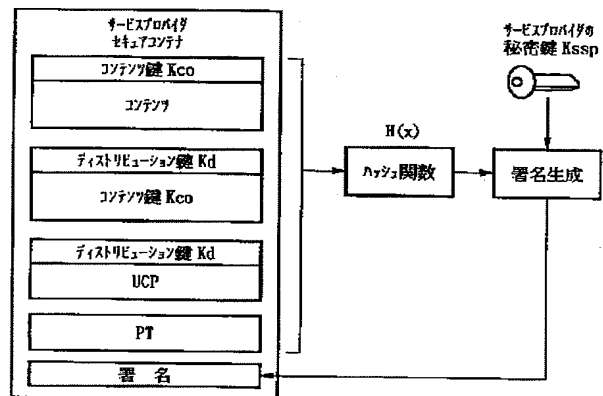
34

体、710…EMD系メディア、720…SCMS系メディア、722…ROM領域、724…セキュアRAM領域、726…RAM領域、800…決済機関

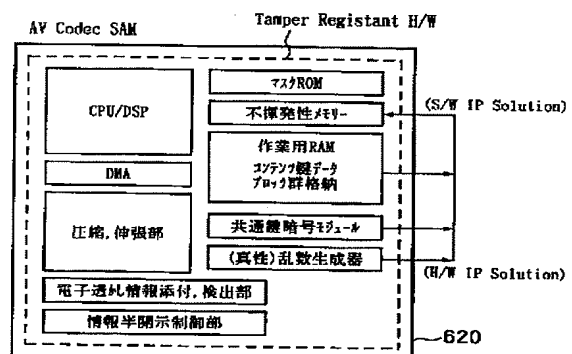
【図22】



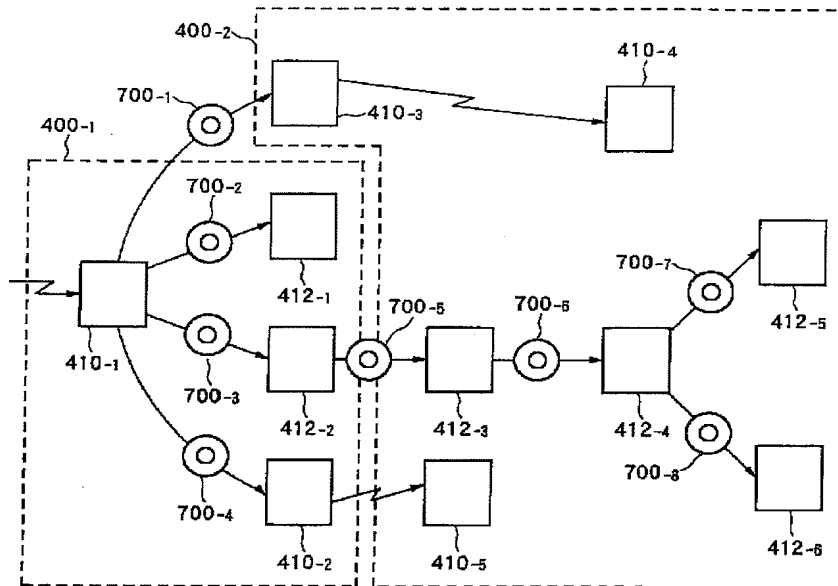
【図3】



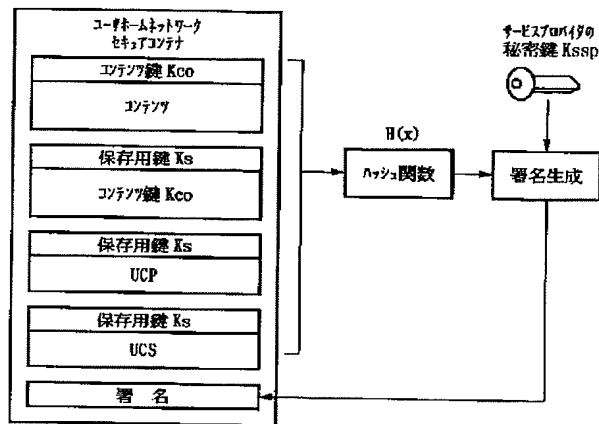
【図12】



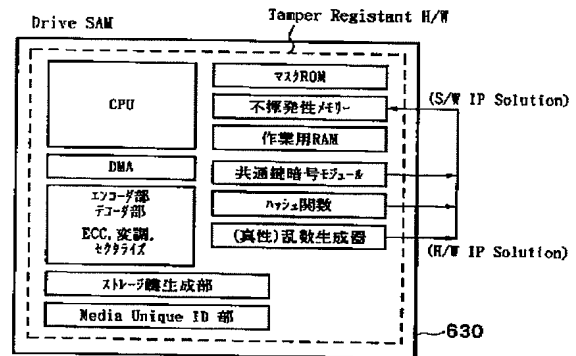
【図4】



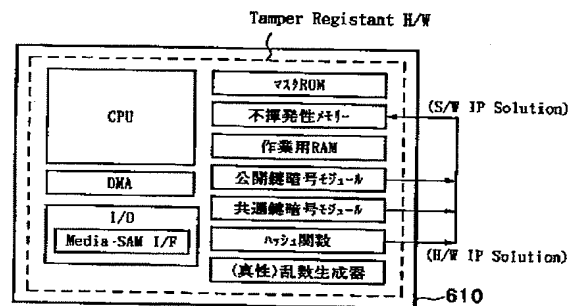
【図5】



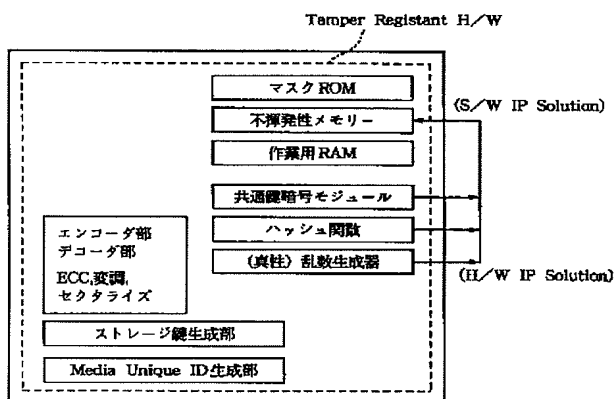
【図13】



【図15】



【図14】



【図6】

## Usage Control Policy(UCP)

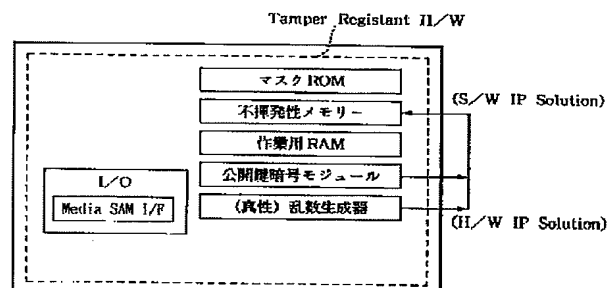
バージョン(Version NO.)
コンテンツプロバイダ アセットマネジメント管理用コンテンツID
署名(コンテンツプロバイダ秘密鍵)
第3信頼機関管理用グローバルユニークコンテンツID
署名(第3信頼機関の秘密鍵)
国、エリアコード
作成者情報 Content Provider ID
作成年月日 Authoring Date
発行者情報:第3信頼機関情報
発行年月日 Issue Date
有効期限 Expiration Date(Validity)
第3信頼機関の通信アドレス
配信サービス事業者情報 Service Provider ID
コンテンツの種別情報① 映画/音楽/番組/CM/宣材
コンテンツの種別情報② 原作/2次利用/編集著作物
コンテンツの表現種別情報① 動画、静止画、音声他、
コンテンツの表現種別情報② 信号諸元、圧縮方式
利用空間調査による取扱制御情報
コンテンツプロバイダによるアクセス制御情報
ユーザによるアクセス制御情報(初期値)
マレージ、割引き引き率に関する取扱方針
推薦決済手段 第3信頼機関/電子マネー決済
試聴モサンプルの取扱制御情報(半開示パラメータ)
コンテンツ(商品)の販売機関/販売国、エリアコード
Usage Control
各購入形態における価格、卸売価格
プロモーション用無料サービス期間/回数
再配付 Re-Distribution
再生課金 Pay-Per-Use 上限回数(→Sell Through) 1回/2回/... n回の価格
買い切り Sell Through
①完全
②期限制限 Time Limited
③回数制限 Pay Per Play N
買い切り Sell Through-SCMS
コピーガード/コピー回数/コピー不可/コピー回数済
記録課金 Pay Per SCMS Copy N
コピーコントロール付 購入枚数
時間(毎)課金 Pay Per Time
ブロック単位課金 Pay Per Block
SCMS機器との互換性 ①EMD →SCMS
②SCMS →END

【図7】

## Usage Control Status(UCS)

コンテンツプロバイダ アセットマネジメント管理用コンテンツID CP_Content ID for Asset Management
署名(コンテンツプロバイダ秘密鍵)
第3信頼機関管理用グローバルユニークコンテンツID CA_Content ID(Globally Unique)
署名(第3信頼機関の秘密鍵)
配信サービス事業者情報 Service Provider ID
配信サービス名
サービスプロバイダ配信サービス管理用コンテンツID SP_Content ID for Delivery Service
署名(サービスプロバイダ秘密鍵)
発行者情報 HNG-ID/SAM_ID/Media SAM_ID
購入者情報 UserID
購入者選択した決済手段 第3信頼機関/転々流通(電子マネー)
購入者決済手段情報 ①銀行、登録講座 ②クレジット会社 ③クレジットカード番号
購入履歴情報
(1回目購入) 購入日付/購入者情報/発行者情報 購入機器情報/購入媒体情報 他
(2回目購入) 購入日付/購入者情報/発行者情報 購入機器情報/購入媒体情報 他
...
(n回目購入) 購入日付/購入者情報/発行者情報 購入機器情報/購入媒体情報 他
コンテンツ販売価格 PT(Price Tag)
購入、利用時の国、エリアコード
利用空間調査情報(各エンティティのIDリスト)
配信サービス内で購入者所持のディスク割付情報 (マレージ/割引き引き率)
コンテンツ単位の購入、利用における購入者、利用者が 所持するディスク割付情報 (マレージ/割引き引き率)
Usage Control
再生課金 Pay-Per-Use 上限回数(→Sell Through) 1回/2回/... n回の価格

【図16】



[illegible]

414

The diagram illustrates two data flow scenarios between Hardware and Media:

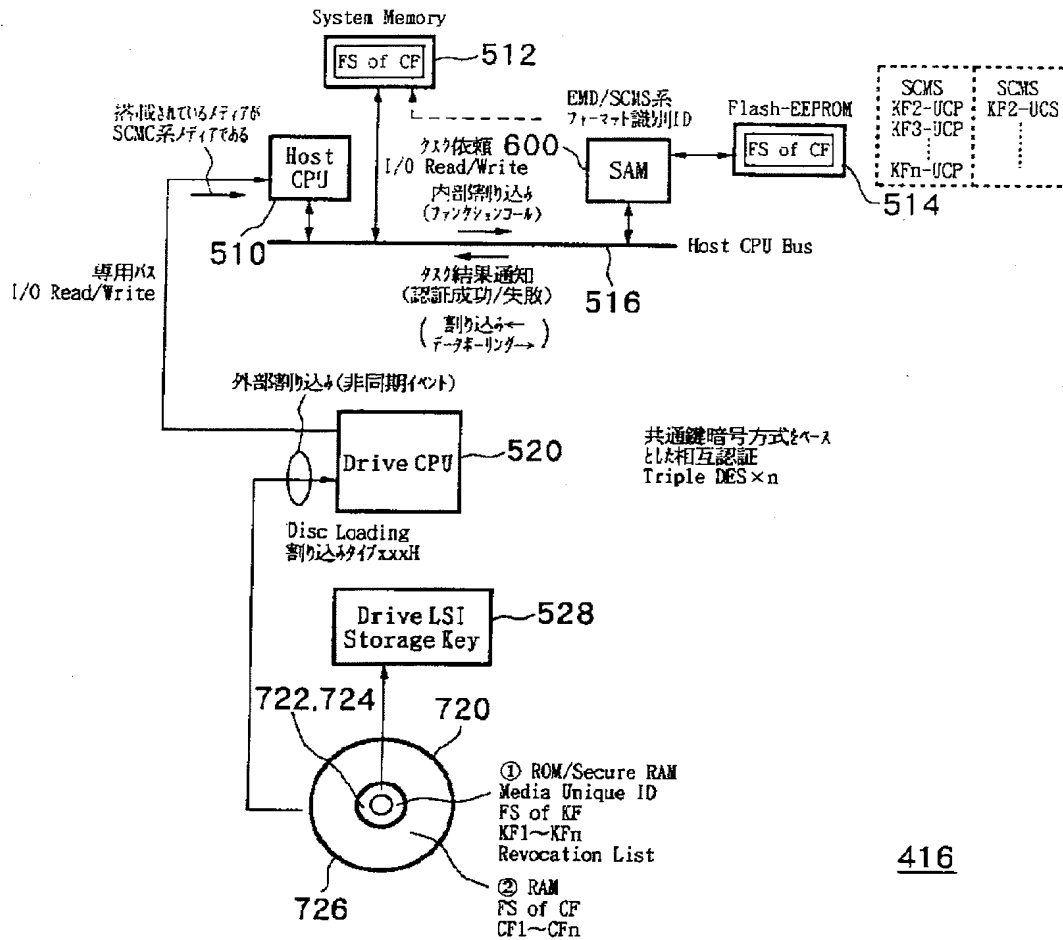
- Left Scenario (再生):** A square labeled 'Hardware' contains a circle labeled '(再生)'. Below it is a circle labeled 'Media'. A solid double-headed arrow connects the Hardware and Media circles, with the label '利用空間調査' (Utilization space investigation) to its left.
- Right Scenario (記録):** A square labeled 'Hardware' contains a circle labeled '(記録)'. Below it is a circle labeled 'Media'. A solid double-headed arrow connects the Hardware and Media circles, with the label '利用空間調査' (Utilization space investigation) to its right.
- Inter-Scenario Flow:** Between the two Hardware squares, there are two horizontal arrows: a top arrow pointing right labeled '再生出力' (Regeneration output) and a bottom arrow pointing left labeled '利用空間調査' (Utilization space investigation).

```

graph TD
    S140([ファイルシステム(コンテナの物理アドレス情報)の上位への転送、設置処理スタート]) --> S141[Drive CPUのRAM、その媒体上の物理アドレス情報を管理するコンテナのファイルシステムを读出して媒体から読み出す]
    S141 --> S142[Drive CPUとHost CPUへ、コンテナのファイルシステムを転送する]
    S142 --> S143[Host CPUへ、システムメモリ展開する]
    S143 --> S144([エンド])
  
```

FIG. 1 is a flowchart illustrating the process of transferring a file system. The process starts at S140, where the file system (physical address information of the container) is transferred to the upper level and the installation process starts. It then proceeds to S141, where the Drive CPU reads out the file system managed by the container from its RAM and the medium. Next, at S142, the file system is transferred from the Drive CPU to the Host CPU. Finally, at S143, the system memory is expanded on the Host CPU, and the process ends at S144.

【図9】



416

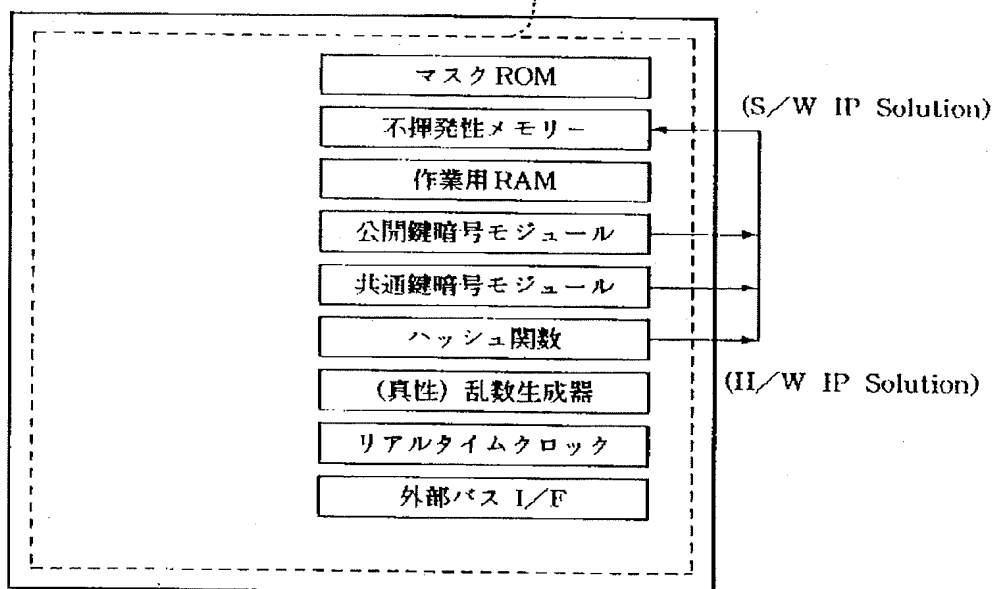
【図19】

ホストネットワークでの利用空間調査 (1対同時多)

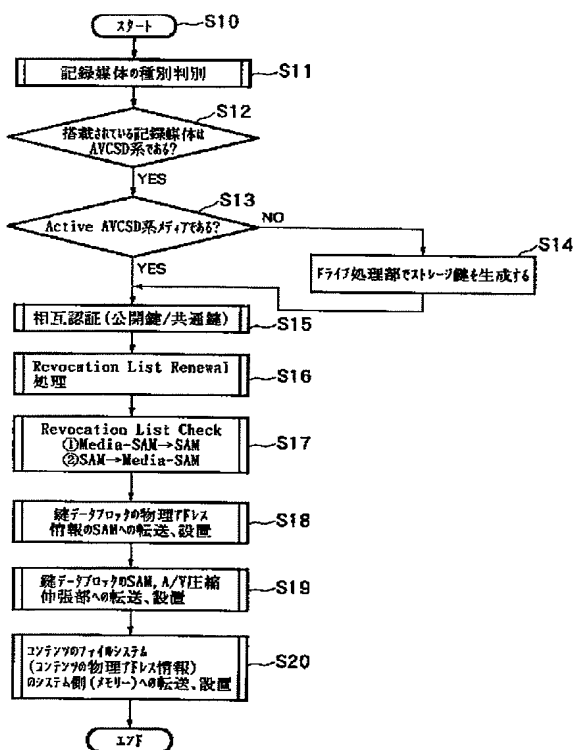
コピックUPC	再生機器	再生メディア	記録機器1	記録メディア1	記録機器2	記録メディア2-1	記録メディア2-2	記録メディア2-3

【図11】

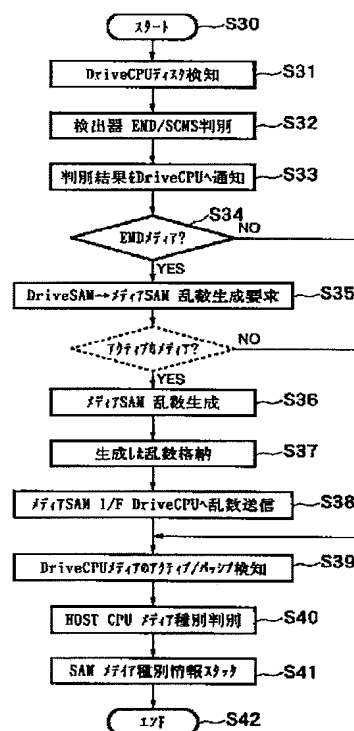
## Tamper Registant H/W



【図20】



【図21】



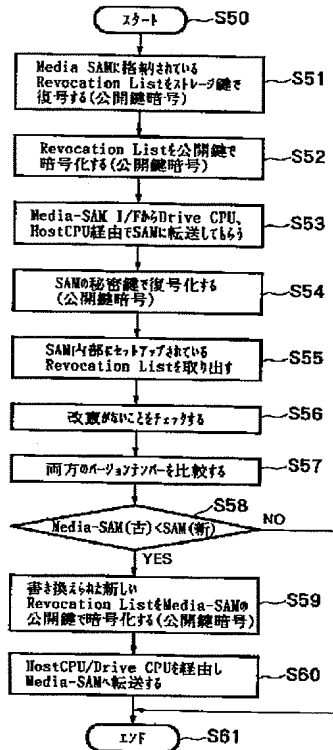


【図18】

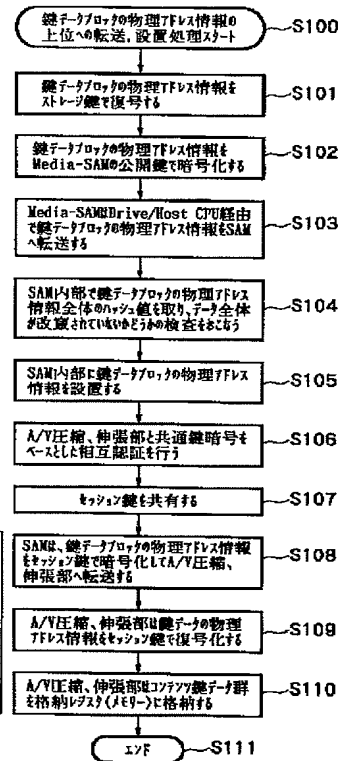
## 利用空間テーブル

コンテンツ 使用許諾条件 UCP/UCS, U-TOC	
EMD系コンテンツ/SCMS系コンテンツ U-TOC コンテンツの権利処理 UCP 信号諸元、圧縮チェック方式 UCP 推奨するものの表示機能 UCP 個人情報(購入者情報) UCS 権利処理(利益分配)データ UCS 関連エンティティ ID Content Provider ID Service Provider ID 第3信頼機関ID	
再生機器 HNG-ID	再生機器に搭載されているメディア
EMD系機器/SCMS系機器 ビットストリームコーデック/否 信号諸元 圧縮コーデック方式 接続するものの表示能力 フォーマット変換機能 有/無 (有の場合、どのような変換機能を保持しているか?) eg. 1bit, 1.2882M→16bit, 44.1K 権利処理(利益分配)用データ 関連エンティティ ID 機器ID 機器開発メーカーID その他利益分配に付関連エンティティ ID 登録している第3信頼機関ID	EMD系メディア/SCMS系メディア メディアタイプ ①メディアの種類 ②ROM/RAM 権利処理(利益分配)用データ 関連エンティティ ID 媒体ID 媒体開発メーカーID その他利益分配に付関連エンティティ ID 登録している第3信頼機関ID
記録機器 HNG-ID	記録機器に搭載されているメディア
EMD系機器/SCMS系機器 ビットストリームコーデック/否 信号諸元 圧縮コーデック方式 接続するものの表示能力 諸元変換機能 有/無 (有の場合、どのような変換機能を保持しているか?) eg. 1bit, 1.2882M→16bit, 44.1K 権利処理(利益分配)用データ 関連エンティティ ID 機器ID 機器開発メーカーID その他利益分配に付関連エンティティ ID 登録している第3信頼機関ID	EMD系メディア/SCMS系メディア メディアタイプ ①メディアの種類 ②ROM/RAM 権利処理(利益分配)用データ 関連エンティティ ID 媒体ID 媒体開発メーカーID その他利益分配に付関連エンティティ ID 登録している第3信頼機関ID

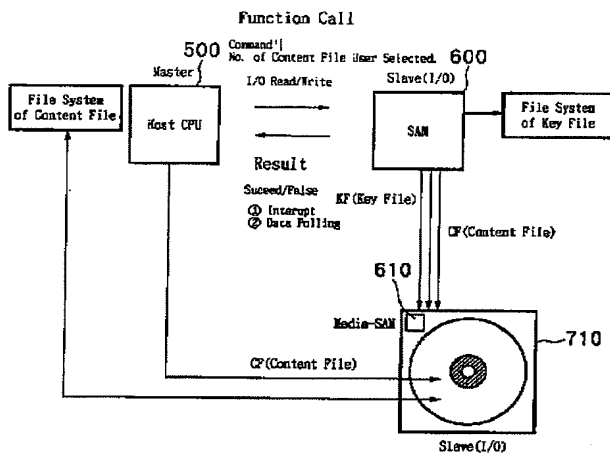
【図23】



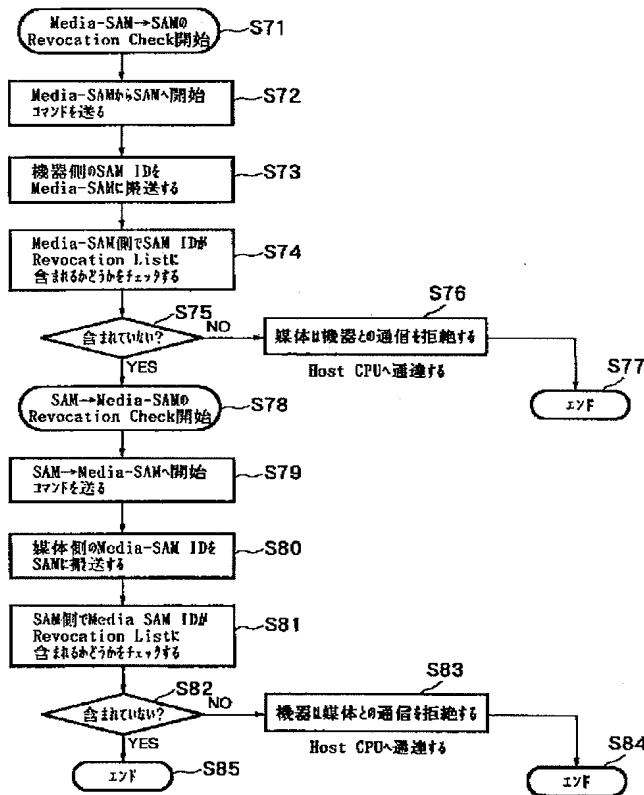
【図25】



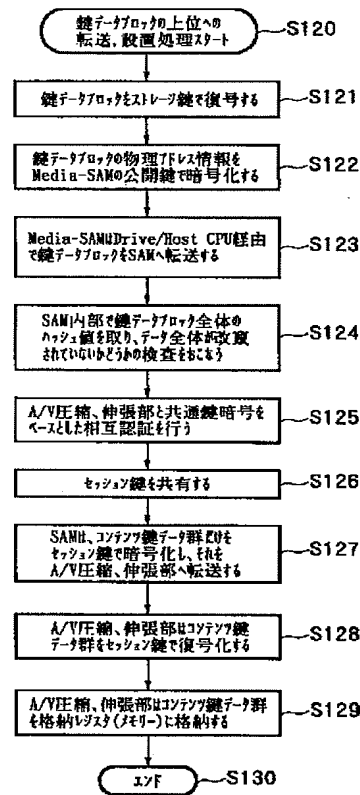
【図28】



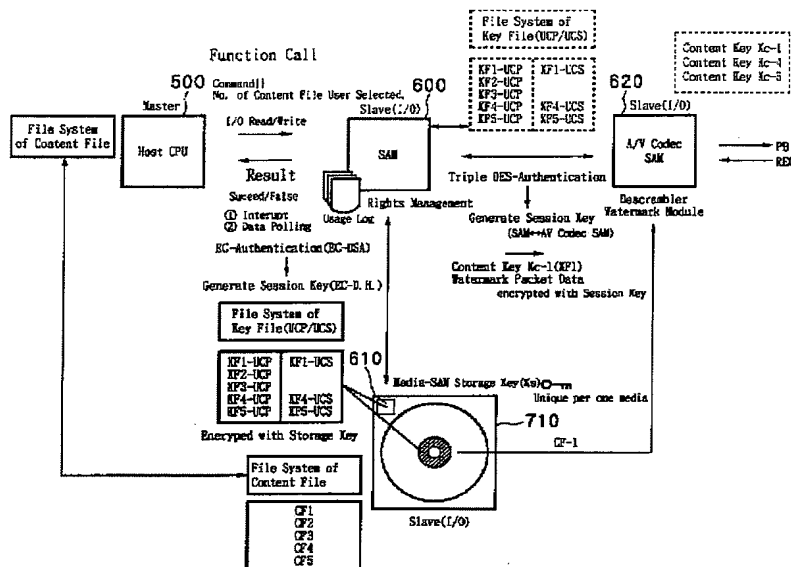
【図24】



【図26】



【図29】



【図43】

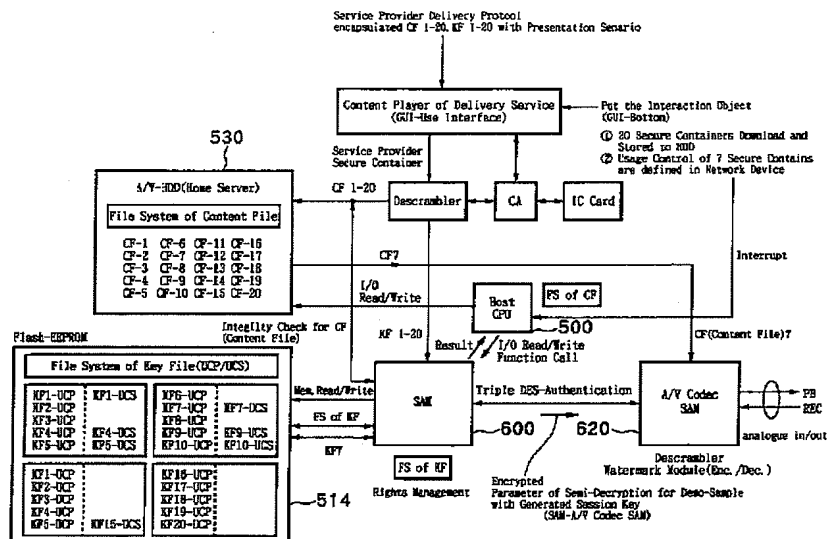
Content ID  
User ID  
Home Network Group ID  
SAM ID  
Purchase/Usage mode: Sell Through  
Price Tag 3

area-code  
discount information

Content Provider ID	xxx
Service Provider ID	xxx
E.M_Place ID	xxx
H/W Provider ID	xxx
Media Provider ID	xxx
Component Provider ID	xxx
Licence Holders ID	xxx
Each Entities ID	xxx
ESC ID	xxx
User ID	xxx

1bit, 2.8224MHz →  
16bit, 44.1KHz, ATRAC2  
SACD → MD

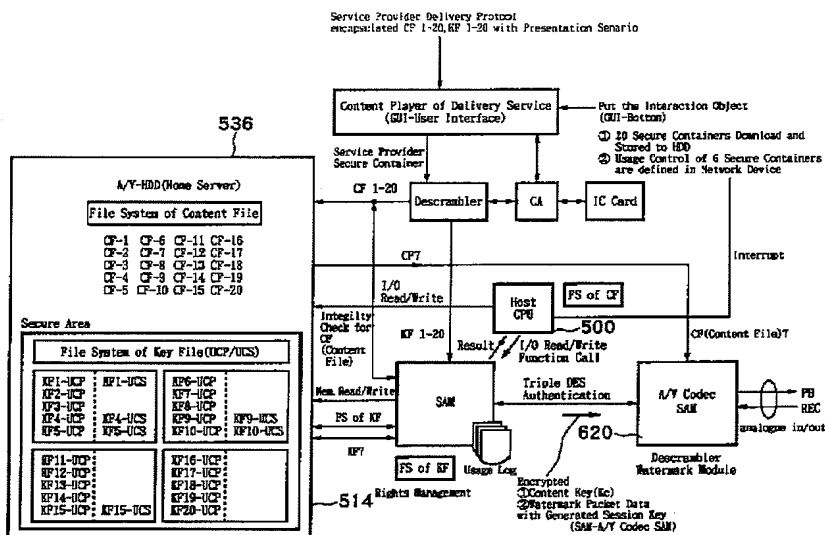
【図30】



【図45】

Content Provider	%
Service Provider	%
Portal (E.M_Place)	%
II/W Provider	%
Media Provider	%
Component Provider	%
Licence Holders	%
Each Entities	%
ESC Charge Fee	%

【図31】

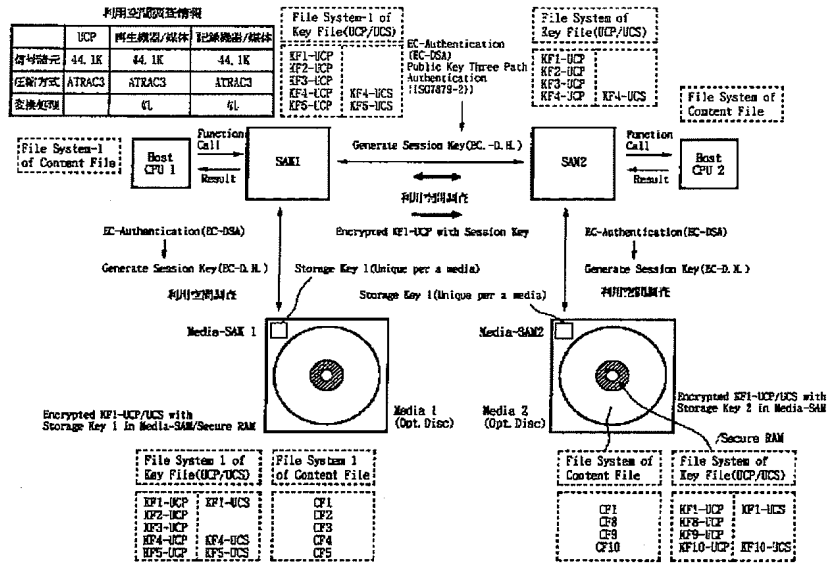


【図46】

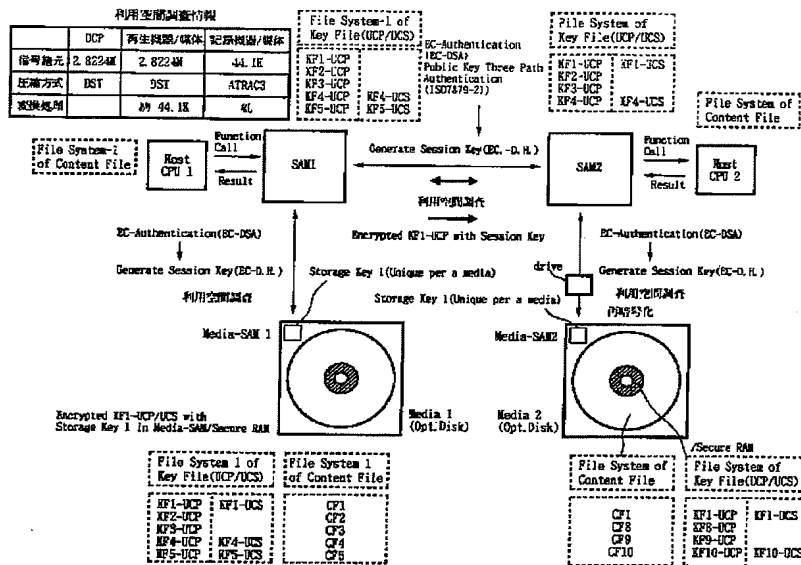
XYZ account no.	XXX	Sell Through	Price Tag 5	×	XYZ	%
PQR TV account no.	XXX				PQR TV	%
ABCD portal account no.	XXX				ABCD portal	%
ABCD account no.	XXX	Pay Per Play × Times	Single × Usage-log	×	ABCD	%
TI account no.	XXX				ABCD	%
Licence Holder account no.	XXX				EFG	%
Each Entities account no.	XXX	copyright_fee			Licence Holder	%
cheaninghouse account no.	XXX				Each Entities	%
					ESC Charge Fee	%

[illegible][illegible]

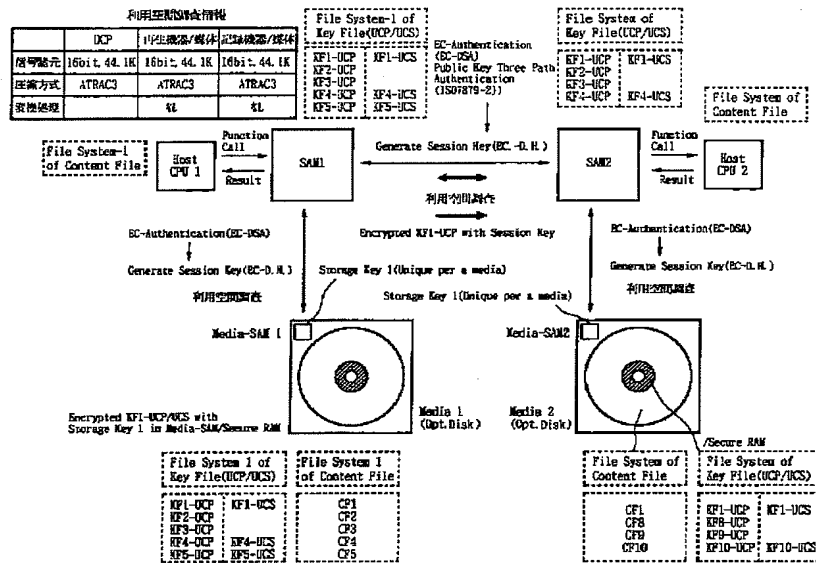
【図34】



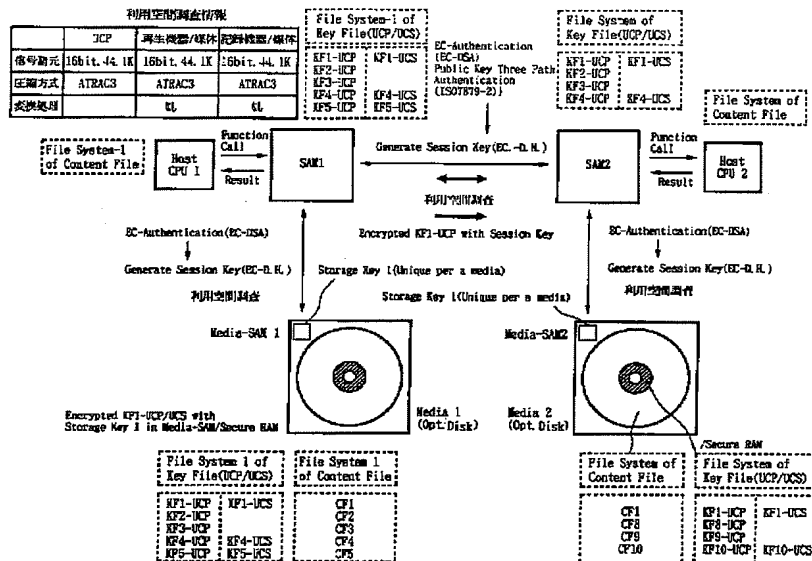
【図35】



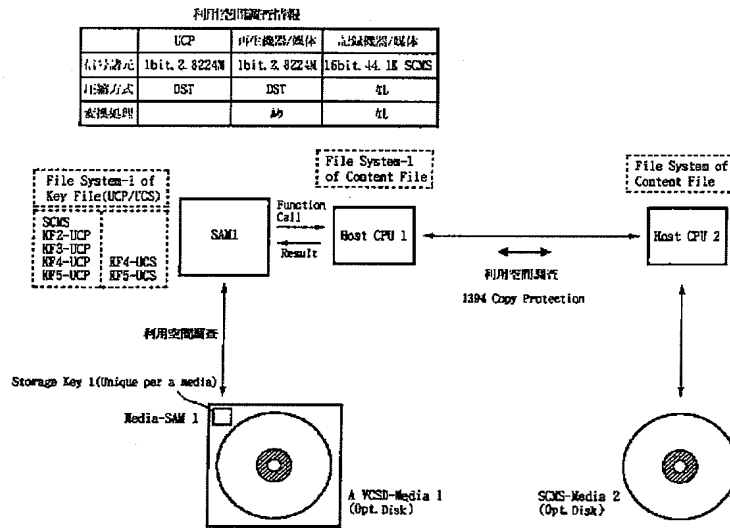
【図36】



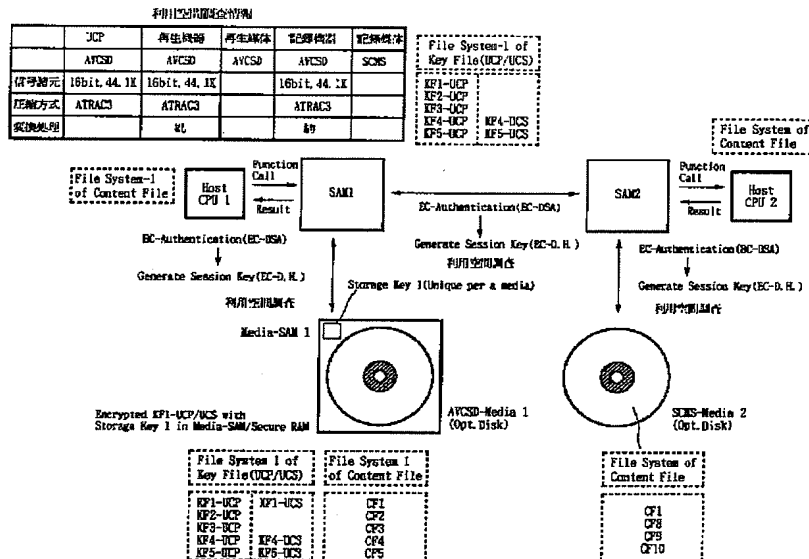
【図37】



【図38】



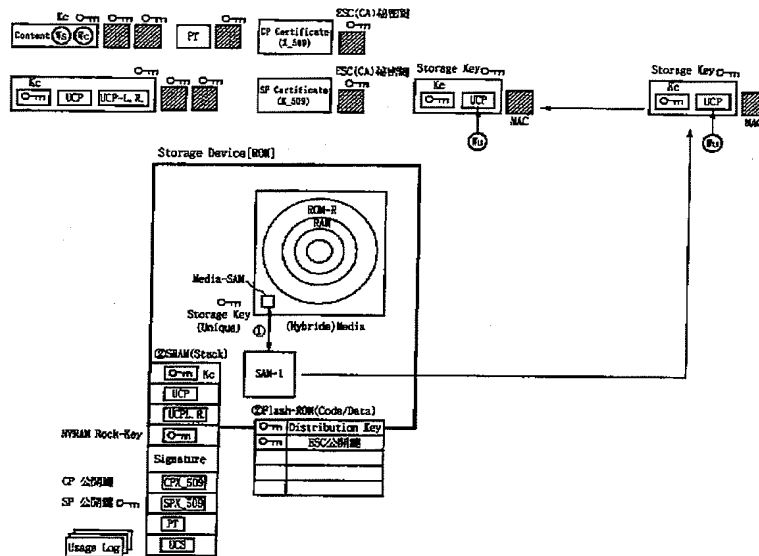
【図39】



[illegible][illegible]



【図42】



【図44】

